FORTRA

Globalscape EFT User Guide

Version: 8.3.0

Copyright Terms and Conditions

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202603311026 - Product Version

Introduction to EFT Managed File Transfer **54**

What's New in EFT? **58**

Feature Availability **61**

Installing EFT and Modules **70**

Before You Begin **71**

System Requirements 72

EFT (Server Service) Requirements 72

EFT Administration Interface Requirements 74

Auditing and Reporting Module (ARM) Requirements 75

AS2 Module Requirements 76

Web Transfer Client (WTC) and Workspaces Requirements 77

Web Admin Client (WAC) Requirements 77

Advanced Authentication Modes Module Requirements 78

Regulatory Compliance Module (RCM) Requirements 78

EFT Outlook Add-In Requirements 79

DMZ Gateway® Requirements 79

Advanced Workflow Module Requirements 79

Remote Agent Module (RAM) Requirements 79

Mobile Transfer Client (MTC) System Requirements 80

Content Integrity Control Action Requirements 80

EFT Specifications 81

Safe Operating Limits 85

EFT System Architecture 86

Installing EFT **87**

Installing EFT, Administration Interface, and Modules 88

Installing the Advanced Workflow Module 103

Installing the Administration Interface Remotely 104

Active-Active HA Cluster—Installing or Upgrading the Server 106

Active-Passive Failover Clustering--Installing or Upgrading 107

Installation Logging 108

Upgrade HA Nodes with Zero Downtime 109

Upgrading EFT and Modules 114

Uninstalling the Software 123

Silent Command-Line Installation **125**

Batch File Examples 126

HA Cluster Example 127

Administration Interface-Only Installation 127

Silent Upgrade 128

Command-Line Parameters 129

Parameter Definitions 129

Registration Parameters 133

135

Debug Logging 135

After You Are Done **136**

Configuration and Security Best Practices 137

Configure the First EFT Connection 138

Creating and Configuring an EFT Server 149
Activating the Software (Licensing EFT and Modules) 150
Registering EFT and the Modules 151
Windows Account for the EFT Server Service 157
Creating a Windows User Account for EFT 158
Set Windows NT Permissions for EFT 160
Assigning the Service to a Windows User Account 163
Backing Up or Restoring Server Configuration 164
Modifying or Repairing the Installation 171
Promoting EFT Stand-Alone to Cluster Node 173
Upgrade HA Nodes with Zero Downtime 174
HA Nodes Configuration Files 179
Administration Interface 181
The EFT Administration Interface 182
Main Menu and Toolbar 185
Server Tab 192
General Tab of a Server 196
Administration Tab of a Server 197
Security Tab of the Server 199
Logs Tab of a Server 200
SMTP Tab of a Server 201
High Availability Tab of a Server 202
Automate Service Account 205

Report Tab of a Server 209
VFS Tab of a Server 210
Status Tab of a Server 212
Status Bar 215
Administration Interface Session Timeout 216
Closing the Administration Interface 218
Configuring Exit Prompts 219
Web Administration Console (WAC) 220
Configure EFT to Use Web Admin 221
Logging In to the Web Admin Console 222
Overview 224
User Management 226
To Create a User 226
To Edit a User 227
To Delete a User 231
Other User Management Options 232
Reset Password 232
Rename 233
Enable 233
Disable 233
Kick 233
Unlock 233
View Site and Node Health 235

View Connected Users ... 236
View Active Automation Rules ... 237
View Transfers ... 238
Administrator Account Configuration ... 239
Administrator Account Security Settings Dialog Box ... 240
Administrator Account Details ... 242
Active Directory-Based Administration ... 243
Creating EFT Administrators ... 245
Administrator Account Permissions ... 250
Optional Permissions for Administrator ... 254
Specifying Administrator Account's Access Rights ... 256
Changing an Administrator Password ... 257
Delegated Administration ... 259
Enforcing Complex Passwords for Administrator Accounts ... 263
Enforcing Password History for Administrators ... 266
Enforcing Password Reset for Administrator Accounts ... 267
Specifying Multifactor Authentication for Admin Accounts ... 269
Expiring Administrator Passwords ... 272
Local Computer Administrators Group ... 274
Locking Out an Administrator Account ... 275
Removing Inactive Administrator Accounts ... 277
Resetting the EFT Administrator Password ... 279
Server Configuration ... 280

Logging In to Administer EFT 281
Logging Out of EFT in the Administration Interface 283
Starting and Stopping EFT 284
Command-Line Login 286
Listening IP Address and Port 288
Specify the Default Time Stamp 291
Deregister Licenses 292
Administering the Server Service 293
Advanced Properties 295
Email Server Settings 299
Configuring Email Server Settings 300
Create a New Secret for OAuth 305
Create Admin Account for OAuth - Microsoft 365 307
Create a Gmail/ Google Cloud Service Account 311
Extending the Trial 318
Connection Problems 320
Specifying a New Local or Remote EFT 321
New Remote EFT Administration Connection 322
Server Groups 328
Renaming, Deleting, and Moving a Server 330
Monitoring Connections to EFT 332
EFT Messages and Templates 333
EmailTemplateVariables 339

File Locations 343
Encryption Algorithms 344
Old Algorithms Removed 345
IPv6 Support in EFT 350
IDN Support in EFT 355
Erasing EFT Configuration 356
HA (Active-Active) Deployments 357
High Availability Overview 358
HA FAQ 360
Non-High Availability mode vs. High Availability mode EFT 365
Non-High Availability Mode vs. High Availability Mode 367
Active-Active HA Cluster—Installing or Upgrading the Server 369
Upgrade HA Nodes with Zero Downtime 370
High Availability-Related COM API Objects 375
High Availability Tab of a Server 376
High Availability Message Queuing 379
HA Nodes Configuration Files 381
Node Discovery Using Shared Storage for HA Clusters 383
EFT System Architecture 386
Server Drain, Maintenance, and Auto-Restart 387
Unicast 388
Viewing Server or Node Status 389
Logging for HA Nodes 391

HA-Related Knowledgebase Articles ... 392

Configuring SSL ... 393

SSL Overview ... 394

Explicit Versus Implicit SSL ... 397

SSL Certificates ... 398

SSL Encryption Algorithms ... 401

SSL Certificate Compatibility ... 404

TLS 1.3 Support ... 405

Assigning a Certificate to an EFT Site ... 411

Certificate Chaining ... 413

Certificate Manager ... 415

Creating SSL Certificates ... 417

Enabling SSL on the Server ... 422

Enabling SSL on the Site ... 424

TLS Settings on the Site ... 425

Configuring SSL Authentication for a Settings Template or User Account ... 427

Exporting a Certificate ... 429

Exporting a Certificate from PFX to PEM ... 430

Importing a Certificate ... 432

Signing a Certificate ... 434

SSL Certificate Expiration Notification ... 436

SSL Certificate-Based Login ... 437

Disabling SSL Connections on the Site ... 440

Using OpenSSL to Generate/Convert Keys and Certificates 441

Federal Information Processing Standard (FIPS) 442

FIPS-Certified Library 443

Enabling FIPS Mode for SSL (HTTPS and FTPS) Connections 446

Enabling FIPS for SSH (SFTP) Connections 447

FIPS Mode Event Messages 449

SFTP FIPS 455

Remote Administration 460

Installing the Administration Interface Remotely 461

Remote Administration 463

Remote Administration FAQ 464

Enabling REST API for Remote Administration 468

IP Access Rules for Remote Administration 470

REST API Support via DMZ Gateway 473

Creating a Remote Connection 474

Configure Remote Administration 481

Starting and Stopping EFT Remotely 483

Remote Administration through DMZ Gateway 485

Introduction to Secure PNC 487

Configuring Secure PNC 488

Configuring Secure PNC using a Self-Signed Certificate 488

Configuring Secure PNC using an EFT Certificate 488

Secure PNC Logging 493

Secure PNC Settings 494

Database Authentication Types 498

Authentication Types 499

Automatically Updating the User Authentication Database 500

Active Directory Authentication 502

Local Security Policy Setting when Using Active Directory Authentication 503

Support for Foreign Groups 507

Removing Domain from the User Folder Name 509

Changing Windows Authentication Options 513

Filter Multiple Active Directory Groups 517

LDAP Authentication 518

Understanding LDAP Authentication 519

Advanced LDAP Filtering 520

Map LDAP Account Attributes to EFT User Account Details 525

Allow AD/LDAP Authentication to EFT through DMZ Gateway 527

Internal Domain Settings 532

Specifying External and Internal Domains 536

Workspaces Invitation and Notification Email Links 538

Map LDAP Users to a Settings Template 540

Connecting to an LDAP Server 542

Changing and Testing LDAP Authentication Options 545

User Home Folders on an LDAP-Authenticated Site 550

Removing Inactive LDAP Accounts from EFT 551

Using Sun Directory LDAP Server 552
ODBC Authentication 553
Using a DSN-Less Connection with ODBC Authentication 554
Changing ODBC Authentication Options 556
Creating Tables for Your ODBC Data Source 557
Script for Creating Necessary ODBC Tables 560
User Home Folders on an ODBC-Authenticated Site 561
Using an ODBC Data Source for User Authentication 562
Establishing a System Data Source Name (DSN) 562
Allow Server to Accept ODBC Database Passwords that are MD5 Hashed 565
EFT Logging and Visibility 566
EFT Transfer Activity Logging 567
EFT Client Activity Log 568
Event Rules Client Log 569
EFT Server Activity Log 572
Log Format, Type, and Location 572
Installation Logging 579
Viewing Connections to a Site 580
Viewing Server or Node Status 581
Viewing Site Statistics 583
Viewing Transfers To and From a Site 585
Performance Counters 589
Site Configuration 594

How EFT Sites are Defined ... 596
Site SettingsTabs ... 598
General Tab of a Site ... 599
Connections Tab of a Site ... 601
Security Tab of a Site ... 603
User Account Details Template ... 605
Content Integrity Control Tab ... 610
Web Tab ... 611
Creating a Site ... 613
Creating an Advanced Security Site ... 635
Propagating an EFT Site ... 646
Starting or Stopping a Site ... 652
FTP/S ... 653
Allowing Site-to-Site Transfers (FXP) ... 654
Allowing Client Anti-Timeout Schemes (NOOP) ... 655
Allowing Multipart Transfers (COMB Command) ... 656
Allowing the Mode Z Command ... 658
Configuring FTP or FTPS ... 659
EFT Support for EBCDIC ... 661
Encoding for FTP Transfers ... 662
File Integrity Checking (XCRC) ... 663
FTP Commands Supported by EFT ... 666
Specifying a PASV IP or PASV Port Range ... 667

Specifying the Value Returned by the FTP SYST Command 668
HTTP/S 669
HTTP and HTTPS Overview 671
Configuring HTTP or HTTPS Transfers 674
Customizable HTTP Error Messages 676
Enable HSTS 677
User Access to the Web Transfer Client 679
Online Certificate Status Protocol (OCSP) 681
OCSP Stapling 682
OCSP Stapling in EFT 682
How can I verify that OCSP stapling in EFT is working? 683
Redirecting HTTP to HTTPS 685
EFT Web Service 687
Using Web Service Examples 693
Using WebDAV in EFT 695
SFTP 698
SFTP Outgoing Ciphers and Advanced Properties 699
Outgoing Ciphers 699
SFTP Encryption Algorithms 704
Enabling SFTP (SSH) on the Server 705
Creating an SSH Key Pair 706
PowerShell Example 710
Available MACs 711

Configuring SFTP for a Site 715
Configuring User SFTP Authentication Options 719
Managing SFTP Keys 721
Encoding for SFTP Transfers 723
Extracting the Public SFTP Key 724
Modifying the SFTP Identification String (Optional) 725
SFTP Key Support 726
SFTP KEX ciphers 728
Specifying SFTP Algorithms 730
SSH Key Formats 731
Using SFTP (SSH) with Radius/RSA SecurID 734
Viewing or Modifying Message Authentication Codes (MAC) Settings 736
AS2 738
Introduction to AS2 739
How EFT Supports AS2 741
AS2 and ARM 745
AS2 Authentication 746
Permutations of Valid Authentication Factors 747
Configuring AS2 Transfers 750
Enabling the AS2 Inbound Listener Service 751
AS2 Certificates 756
Configuring AS2 Partners 757
Editing AS2 Partner Profiles 757

Configuring AS2 Outbound Partners Using the Wizard 759
Configuring AS2 Inbound Partners Using the Wizard 768
AS2 Inbound Parameters 776
AS2 Outbound (Sender) Parameters 780
Configuring an AS2 Outbound Proxy 785
Initiating AS2 Outbound Transactions 786
Moving Files Received from AS2 Partners 787
Renaming Files Received from AS2 Partners 788
AS2 Account Information Web Page 789
Allowing AS2 Connections to a Site 791
Allowing AS2 Connections in the Settings Template or User Account 792
AS2 Events, Conditions, Actions, and Variables 793
Introduction to AS2 Events, Conditions, Actions, and Variables 794
AS2 Events 795
AS2 Conditions 799
Sending Files to an AS2 Partner via Event Rules 800
AS2 Variables 806
AS2 Transaction Auditing and Monitoring 807
Introduction to AS2 Transaction Auditing and Monitoring 808
AS2 Information in the Database 809
AS2 Transaction Reports 810
Transfers - AS2 Status Viewer 811
Customizing the Display 812

Resubmitting AS2 Transmissions 813
AS2 Transaction Success and Failure Notification 814
Testing the AS2 Outbound Connection 815
Troubleshooting AS2 Issues 817
AS2 and the Auditing and Reporting Module 818
AS2 Error Warnings and Prompts 819
AS2 Configuration Errors 819
AS2 Transfer Errors 819
Connection Settings 821
Protocol Settings 822
Connection Banner Message 825
User Limit Reached Message 828
Quit Session Message 829
Content Integrity Control 830
Create a CIC Profile 831
ICAP Options 833
Automatically Creating a Home Folder for New Users (Site) 836
Azure Data Lake Storage 837
Banning Unwanted File Types 838
Changing a Site's IP Address or Port 840
Changing a Site's Root Folder 843
Connection Limits Dialog Box 845
Controlling Access to the Site by IP Address 847

Configuring Azure Key Vault Support for EFT 851
Configuring the Secrets Module 856
Deleting a Site 861
Enabling the Account Management Page 862
Folder Sharing (Workspaces) 864
EFS Encryption 869
Encrypted Folders (EFT Encryption) 872
Site Encryption 877
Per-Folder Encryption 877
User-Specific Encryption 878
Enabling EFT-Managed Encryption 878
Flooding and Denial of Service Prevention 882
Flood and DoS Prevention Scoring 883
Customizations 886
Internal Domain Settings 888
Specifying External and Internal Domains 892
Workspaces Invitation and Notification Email Links 894
Override VFS Credentials 896
Proxy Protocol 900
Renaming a Site 904
Runtime Template Variables 905
Searching a Site 907
Setting Maximum Concurrent Socket Connections 910

Setting Maximum Concurrent Logins 913
Setting Maximum Connections per User 914
Setting Maximum Connections per IP Address 915
Setting Maximum Transfers per Session 916
Setting Maximum Transfer Size 917
Setting Maximum Transfer Speeds 919
Specifying File Deletion Options 921
Unicode Exceptions 923
Unicode File Transfers 928
Unicode FAQs 929
User Database Refresh 933
Controlling Access to Folders (Permission Groups & VFS) 935
Introduction to Permission Groups - Controlling Access to Folders 936
Introduction to the Virtual File System (VFS) 939
How VFS Permissions Work 941
Adding a User or Group to VFS Permissions 946
Adding or Removing Users to or from a Group 950
Creating a New Physical Folder 952
Creating a New Virtual Folder 953
Creating Permission Groups 955
Deleting Groups 956
Deleting a Physical Folder 957
Deleting a Virtual Folder 958

Disabling Inheritance in the VFS 959
Encrypted Folders (EFT Encryption) 961
Site Encryption 966
Per-Folder Encryption 966
User-Specific Encryption 967
Enabling EFT-Managed Encryption 967
EFS Encryption 971
Mapping a Virtual Folder to a Network Drive 974
Renaming a Group 975
Renaming a Physical Folder 976
Renaming a Virtual Folder 977
Resetting VFS Folder Permissions 978
Setting VFS Permissions 979
Specify Upload Quota in the VFS 981
Viewing Group Membership 985
WTC Users in the VFS 986
Settings Template Configuration 987
How Settings Templates Work 988
Settings Template Tabs 989
General Tab of the Settings Template 990
Connections Tab of the Settings Template 991
Security Tab of the Settings Template 993
Creating or Deleting Settings Templates 994

Inheritance ... 996
Settings Template Home Folder ... 997
Enabling or Disabling a Settings Template ... 998
Moving a User to a Different Settings Template ... 999
Guest Users Settings Template ... 1000
User Account Configuration ... 1003
Anonymous User Accounts ... 1005
Banning an IP Address that Uses an Invalid Account ... 1006
Configuring User Account Details ... 1008
User Accounts ... 1010
General Tab of a User Account ... 1011
Connections Tab of a User Account ... 1013
Security Tab of a User Account ... 1015
User Icons ... 1016
Creating a User Account ... 1017
Deleting a User Account ... 1024
Deleting or Disabling Inactive User Accounts ... 1025
Disconnecting Users after a Defined Number of Invalid Commands ... 1027
Disconnecting Users on Timeout ... 1028
Enabling or Disabling a User Account ... 1029
Expiring a User Account ... 1030
Forcibly Logging a User Off of EFT (Kick User) ... 1031
Generating a List of Expired User Accounts and Expiration Dates ... 1032

Managing Multiple User Accounts ... 1035
Specifying User Disk Quota ... 1036
Specifying a Home Folder ... 1039
Specifying a User's Permission Group ... 1042
Specify GDPR Status, Privacy Policy Options, and Terms of Service for Users ... 1044
Specifying the Home Folder for AD-Authenticated Users ... 1047
Unlocking a User Account ... 1048
Updating a User Account's Email Address ... 1049
User Login Credentials Message ... 1050
Username Resend Message ... 1053
Users are Unable to Upload/Download in Home Directory ... 1054
Viewing a User's Home Folder ... 1055
Viewing User Statistics ... 1058
Password Security Settings ... 1060
Emailing Users' Login Credentials ... 1061
Changing a User's Password ... 1062
Encrypting Passwords ... 1064
Enforcing Complex Passwords ... 1065
Expiring Passwords ... 1068
Important: Effect of Settings Changes and Template Reassignment on Password Expiration ... 1068
Applying Changes to Password Expiration Settings ... 1068
Moving a User to a Different Settings Template ... 1068
Administrative Considerations ... 1069

AD Password Expiration **1072**

Password Reset Messages **1073**

Allowing or Forcing Password Reset **1076**

Disabling or Locking Out an Account **1079**

Prohibiting Password Reuse **1081**

Reminding Users when Password is About to Expire **1084**

How are Passwords Stored in EFT? **1086**

Advanced Authentication Modes Module (AAMM) **1087**

Introduction to the Advanced Authentication Modes Module 1088

OpenID Configuration 1090

RSA SecurID Supported Features 1094

Configuring RSA SecurID Support on an Existing Site 1095

RADIUS for User Authentication 1098

Configuring RADIUS Support on an Existing Site 1103

Enabling or Disabling RSA Authentication via RADIUS 1106

SAML (Web SSO) Authentication 1107

Introduction to SAML (Web SSO) Authentication 1108

Configuring a Site for SAML (Web SSO) Authentication 1112

SAML Scope 1119

SSO Process 1121

Tools for Debugging SAML Communications 1124

Validate Username Regex 1124

Generate SP Metadata File 1126

Web SSO Error Handling 1129
Related Knowledgebase Articles 1130
Common Access Card Authentication 1131
Configuring CAC on an LDAP Site 1134
Advanced Workflow Module 1135
What's New in the AWM? 1136
Installing the Advanced Workflow Module 1142
Upgrading the Advanced Workflow Module 1143
Automate Service Account 1148
Introduction to Advanced Workflows 1152
Workflow Concepts 1154
The Workflow Task Builder Overview 1156
Task Builder Interface 1158
Adding Task Steps 1160
Editing Task Steps 1162
Editing Step Properties 1163
Moving Steps 1164
Indenting Steps 1165
Disabling, Enabling, or Deleting Task Steps 1165
Step Numbers & Word Wrap 1166
Switching from Visual to the AML View 1166
Undoing and Redoing Changes 1167
Copying and Reusing Task Steps 1168

Finding and Replacing Text in Task Steps 1171
Task Builder File Menu 1181
Task Events 1184
Task Functions 1186
Actions 1192
Actions Panel 1203
Finding & Organizing Actions/ Activities 1209
My Actions 1211
Action Properties 1214
Task Builder Options 1216
Task Builder Toolbar Options 1217
Task Builder General Options 1219
Task Builder Formatting Options 1224
Task Builder Font Options 1227
Task Builder Color Options 1229
Task Builder Layout Options 1234
Task Builder Debugger Options 1235
Task Builder Ribbon 1238
Task Builder Status Bar 1252
Task Builder Steps Panel 1254
Custom Step Description 1257
Percent Signs in Advanced Workflows 1259
Testing Tasks Using Run Options 1261

Task Variables 1265
Creating and Defining Task Variables 1267
Editing and Deleting Task Variables 1267
Creating Variables (Advanced Workflow Module) 1269
Error Causes 1273
On Error 1279
Error Handling 1285
Debug Panel Overview 1287
Task Builder Debugger Options 1288
Debugging Tools 1291
Debug Panel - Output 1292
Debug Panel - Variables 1295
Debug Panel - Breakpoint 1299
Setting Breakpoints 1300
About Bookmarks 1302
Debug Panel - Watches 1304
Using Watches 1305
Debug Panel - Labels 1307
Debug Panel - Attachments 1309
Adding Attachments 1312
Debug Panel - Comments 1314
Adding Comments 1315
Debug Panel - Call Stack 1316

Debug Panel - Regions 1317
About Regions 1318
Debug Panel - Sessions 1321
Advanced Workflow Module Features and Benefits 1322
Creating Workflows for Use in an Event Rule 1325
Creating Advanced Workflow Folders 1328
Adding a Workflow Action to an Event Rule 1329
Enable or Disable Running Task Window 1332
Sample Workflows 1334
Advanced Workflow Variables 1336
Advanced Workflow Conditions 1337
Backing Up Advanced Workflows 1338
Importing and Exporting Advanced Workflows 1339
Encrypt Files in a Workflow Using EFT OpenPGP Key 1341
Technical Reference 1342
Introduction to AML (Automation Markup Language) 1343
Arrays 1344
What are Constants? 1346
Datasets 1347
Expressions 1352
Functions and Extended Functions 1354
Event Rules (Automation) 1357
Introduction to Event Rules 1358

Transferring Files with Event Rules 1362
Event Rules Modules 1363
Propagating Event Rule Artifacts 1365
Event Rules Client Log 1370
Connection Profiles 1373
Introduction to Connection Profiles 1374
Defining a Connection Profile 1375
Creating Event Rules 1384
Defining Event Rules 1385
Event Rule Folders 1390
Event Rules Change Log 1391
Using Virtual Paths In Event Rules 1394
Using Login Credentials in Event Rules 1397
Using Run Now to Test an Event Rule 1398
Exporting and Importing Event Rules 1400
Managing Event Rules 1402
Event Rule Permissions 1405
Advanced Transfer Options 1411
Event Rule Load Balancing 1417
SSL Options Dialog Box 1419
Propagating Event Rule Artifacts 1421
Logging Event Rule Transfer Failures 1426
Changing the Number of Concurrent Threads Used by Event Rules 1427

Too Many Connections per Site 1428
Applying a Rule to a Specific User or Group 1429
Example: Copying or Moving a File Triggered on Monitor Folder Event and Renamed 1430
Example: Send an Email Notification When a Certain User Uploads a File 1431
Example: Copy/Move and Download File Cloud Storage Actions 1432
Example: Copying Folder Structure When Offloading Files 1435
Example: Moving an Uploaded File Based on Filename 1436
Proxy Settings 1439
Defining a Proxy 1440
Configuring Advanced Proxy Settings 1443
Using a SOCKS Proxy Server 1446
Routing Outbound Traffic through a Proxy 1448
EFT Variables 1449
How to Use the Variables 1451
Advanced Workflow Variables 1453
AS2 Variables 1454
Cloud Variables 1455
Connection Variables 1456
Event Properties Variables 1457
File System Variables 1459
Remote Agent Context Variables 1463
Scheduler (Timer) Rule Variables 1464
Server Variables 1465

Site Variables 1466
Transfer Properties Variables 1467
User Variables 1468
Workspaces-Related Variables 1472
Using Context Variables for Parameterized Event Rules 1473
Events (Triggers) 1475
Event Triggers 1476
AS2 Events 1482
Cloud Object Monitor Event 1486
Connection Events 1488
Event Rule Subroutine Event 1489
File System Events 1490
File Uploaded Event 1519
Folder Monitor Event 1521
GDPR Right Exercised 1531
IP Added to Ban List Event 1532
Operating System Events 1533
REST Invocation Event 1537
Scheduler (Timer) Event 1545
Secure File Send Events 1549
Server Events 1551
Site Events 1554
User Events 1555

Workspaces Events 1559
Actions 1560
Available Actions 1562
Order in which Actions are Executed 1565
Order in which Event Rules are Executed 1567
Adding an Action to an Event Rule 1570
Which Actions are Available with Which Event Triggers? 1571
Cryptography: OpenPGP Configuration 1573
OpenPGP and EFT 1574
OpenPGP Encryption Algorithms 1577
Creating Key Pairs for OpenPGP 1578
Setting OpenPGP Security for the Site 1583
The OpenPGP Keyring Manager 1585
Removing OpenPGP Key Pairs 1587
Importing and Exporting Key Pairs 1588
Cryptography: OpenPGP Action 1590
OpenPGP on File Upload Event Rule 1595
Cryptography: OpenSSL Action 1596
Cloud Download and Upload Actions 1599
Cloud: REST-Web Services Action 1602
Azure Data Lake Storage 1606
EFT Web Service 1607
Using Web Service Examples 1613

Compression Action 1615
Export to Dataset and Import CSV from Dataset Action 1618
File Operation Action 1620
File: Scan Action 1628
Content Integrity Control 1629
Content Integrity Control Tab 1631
How does File: Scan Work in Event Rules? 1632
Scan a File Using the File: Scan Action 1633
Scanning Metadata 1638
File Scan Action Example 1639
Flow: Abort User Operation 1648
Flow: Stop Processing Action 1649
Flow: Subroutine Action 1651
Flow: Variable Action 1655
Folder: Operation Action 1657
Pre and Post Commands 1658
Datasets in Event Rules 1660
Loop: Dataset and Loop Break Action 1668
Protocol: Listing to Dataset Action 1670
Protocol: AS2 Action 1674
Sending Files to an AS2 Partner via Event Rules 1675
AS2 Information in the Database 1681
AS2 Transaction Reports 1682

Transfers - AS2 Status Viewer 1683
Customizing the Display 1684
Resubmitting AS2 Transmissions 1685
AS2 Transaction Success and Failure Notification 1686
Protocol: Download Action 1687
Protocol: Email Action 1692
Creating an Email Notification Template 1696
Protocol: Synchronize Action 1698
Protocol: Upload Action 1703
Adding a Workflow Action to an Event Rule 1710
Script: Custom Command Action 1713
Custom Commands 1714
Creating a Command with the Custom Command Wizard 1715
Editing a Command 1719
Custom Command Example 1722
Viewing and Deleting Commands 1726
Enabling and Disabling Commands 1727
Command Permissions 1728
Using the "Script: Custom Command" Action 1729
Example: Using a Command in an Event Rule to Copy Files 1732
Script: PowerShell Action 1735
Smart Overwrite 1737
System: Backup Action 1739

System: Cleanup Action 1742
System: Report Action 1744
User Action 1748
User Create Action 1750
Using Wildcards with Event Rule Actions 1751
Windows Event Log (WEL) Action 1753
Conditions 1755
Using Conditions 1756
Condition Placement 1758
Changing Condition Placement 1760
Condition Evaluation 1762
Else Clauses 1763
Logical Operators 1764
Evaluating Expressions in Event Rules 1767
Compound Conditional Statement 1768
Event Properties 1770
Advanced Workflow Conditions 1773
AS2 Conditions 1774
Connection Conditions 1775
Context Variable Condition 1778
File System Conditions 1779
Remote Agent Event Rule Conditions 1787
Secure Message Conditions 1788

Server Conditions 1790
Site Conditions 1794
User Conditions 1795
Workspaces Conditions 1807
Auditing and Reporting Module 1810
Introduction to the Auditing and Reporting Module 1811
Installing and Configuring Auditing and Reporting 1812
Activating the Auditing and Reporting Module 1815
Auditing and Reporting Interface 1816
ARM Database 1817
EFT Database Utility 1818
EFT DB Files 1827
Database User Account Privileges 1830
ARM Database Maintenance 1832
Upgrading the EFT Database 1835
Upgrading a Large Database 1843
Manually Creating the ARM Database in SQL Server 1845
Manually Creating the ARM Database in Oracle 1851
Purging Data from the Database 1856
Auditing 1857
Audit Database Settings 1858
Auditing Database Recovery 1861
Fact Tables 1862

Refreshing the FACT Tables ... 1864
How EFT Handles SQL Data ... 1865
Auditing Event Rule Actions ... 1866
Auditing Administrator Changes to the ARM Database ... 1867
Result IDs ... 1870
Auditing Database Errors and Logging ... 1873
ARM Database Schema Change Tracking ... 1875
Security Auditing ... 1876
PCI DSS Compliance Report ... 1877
Automating the Compliance Report ... 1879
PCI DSS Possible Compliance Report Outcomes ... 1880
Reporting ... 1882
Descriptions of Preconfigured Reports ... 1883
Generating a Report ... 1890
Using Report Filters ... 1891
Defining Custom Reports ... 1893
VSReport Designer ... 1894
Opening VSReport Designer ... 1896
Creating a Report with the Report Wizard ... 1898
Creating a Report in Design Mode ... 1904
Changing Field, Section, and Report Properties ... 1907
Adding, Editing, and Deleting Fields in the Report ... 1909
Changing the Data Source ... 1913

Grouping and Sorting Data ... 1916
Example: Creating a Custom Report ... 1918
Managing Reports ... 1923
Saving a Report ... 1924
Exporting Reports in XML Format ... 1925
Exporting and Publishing Reports in the Report Designer ... 1926
Importing Reports ... 1927
Deleting a Report ... 1928
Saving Report Outputs ... 1929
Renaming a Report ... 1930
Regulatory Compliance Module ... 1931
Introduction to the Regulatory Compliance Module ... 1932
GDPR Settings ... 1933
GDPR Data Protection Officer ... 1943
GDPR-DPIA Report ... 1945
Personal Data Encryption ... 1947
Privacy Policy ... 1949
Edit the Privacy Policy and Labels ... 1951
GDPR Right Exercised ... 1952
Terms of Service Agreement ... 1953
Specify GDPR Status, Privacy Policy Options, and Terms of Service for Users 1958
PCI DSS Compliance ... 1962
Payment Card Industry (PCI) Data Security Standard (DSS) ... 1963

How EFT Addresses PCI DSS Requirements 1964
PCI DSS Requirements Addressed 1964
PCI DSS Compliance Report 1969
Automating the Compliance Report 1971
PCI DSS Possible Compliance Report Outcomes 1972
Warnings for PCI DSS Violations 1974
Remote Agent Module 1976
Introduction to Remote Agents 1977
Installing Remote Agents 1979
Remote Agent Updates 1986
Remote Agents License Status 1989
Remote Agent Updates 1992
Remote Agent Templates 1995
Remote Agent Rules 2001
Remote Agent Context Variables 2006
Managing Remote Agents 2007
Sending Files to a Different Server 2010
Remote Agent Logging 2012
Remote Agents in the VFS 2014
Decommissioning a Remote Agent 2015
Web Transfer Client and Workspaces 2016
How Do I Share Files? 2017
WTC and Workspaces User Guide 2019

Overview of the Web Transfer Client 2020
Logging In 2023
Changing Your Password 2027
Sharing Folders (Creating a Workspace) 2028
Stop Sharing a Workspace 2034
Add Workspace Participants 2035
Edit-Remove Workspace Permission 2036
Register a New Account 2038
Downloading Files 2040
Uploading Files and Folders 2042
Resuming Transfers 2044
Canceling a Transfer 2045
Workspace and File Expiration 2046
Creating Folders 2048
Deleting a Folder or File 2049
Change Your Profile 2050
Personal Data & Privacy Settings 2053
Drop Off Page 2058
Pick Up Files 2061
Reply to Messages 2064
Request Files 2066
Send/Email Files in Workspaces 2069
Viewing Sent Messages 2074

Viewing Received Messages 2076
Viewing Transfer Status 2077
View Workspaces History 2078
Edit Notification Options 2081
Notifications 2083
Messages 2085
Workspaces Comments 2086
File-Naming Conventions 2088
Filtering and Sorting the File List 2089
Moving Files between Folders 2090
Renaming a File or a Folder 2092
Searching for Files 2093
Language Settings 2094
Web Transfer Client Pagination 2095
Logging Out 2096
Automatic Log Out 2096
WTC & Workspaces Administration 2097
Introduction to Workspaces 2098
Workspaces Licenses 2100
WTC Admin-Configuration Settings 2103
Enable HSTS 2104
Allow Users to Create Workspaces 2106
Changing Logo and Colors in the WTC and Login Page 2108

User Access to the Web Transfer Client 2113
Folder Sharing (Workspaces) 2115
Send and Reply Portals 2120
Request File Portal 2125
Drop-Off Portal 2126
Multifactor Authentication for the WTC and Workspaces 2131
Enabling the Account Management Page 2138
Upload Forms (Secure Forms) 2140
Privacy Policy 2144
Edit the Privacy Policy and Labels 2145
Privacy Reports 2147
Display Full Name of User in the WTC 2148
Changing the Language of the Client 2149
Disable CRC 2150
Guest Users 2152
Logging In 2154
Workspaces SSO Authentication 2158
Managing Workspaces in the VFS 2159
Restrict Workspaces Invitations to Specific Domains 2161
Transactional Workspaces 2163
Unicode File Transfers 2165
Unicode FAQs 2166
Workspaces Conditions 2170

Workspaces Invitations 2173
Workspaces Notifications 2176
Workspaces Permissions 2181
Workspaces Permissions on an Active Directory Site 2181
Workspaces-Related Variables 2184
Viewing Data in DB Browser 2185
Using the EFT Outlook Add-In 2188
Introduction to the EFT Outlook Add-In 2189
Installing the EFT Outlook Add-In 2190
EFT Outlook Add-In Interface 2194
Changing the Message Format in Outlook 2195
Connecting to EFT from Outlook 2196
Configuring Message Options in Outlook 2199
Enabling or Disabling the Outlook Add-In in Outlook 2202
Deploy Outlook Add-In on End-User's Computers 2203
Enabling Outlook's Language Detection 2206
Mail Profiles with Multiple Accounts 2207
Recovering an Email from "Unrecoverable Error" 2208
Sending Files with the Outlook Add-In 2209
Viewing Add-In Status 2212
Mobile Transfer Client (MTC) 2214
Mobile Transfer Client Introduction 2215
Enabling and Configuring the Mobile Transfer Client in EFT 2217

Create a Profile 2221
Connecting to EFT 2222
Obtaining the Mobile Transfer Client App 2224
DMZ Gateway 2225
Introduction to DMZ Gateway® 2226
What's New in DMZ Gateway®? 2228
System Requirements for DMZ Gateway 2232
DMZ Gateway Tab - Configuring Perimeter Network Security 2233
Acceleration 2235
DMZ Gateway in EFT 2236
DMZ Gateway Technical FAQ 2239
DMZ Gateway Knowledgebase Articles 2242
Installing DMZ Gateway 2244
Installing DMZ Gateway on a Windows System 2245
Activating DMZ Gateway 2250
Licensing DMZ Gateway for EFT with the Accelerate Module 2250
Activation Interaction between DMZ Gateway and EFT Trial 2251
Installing DMZ Gateway on a non-Windows System 2253
Installing DMZ Gateway on RedHat or SuSE Linux 32-Bit or 64-Bit 2254
Installing DMZ Gateway on Ubuntu Linux 32-Bit or 64-Bit 2254
Solaris x86 32-Bit or 64-Bit 2255
Example of Installation Process on Solaris 2256
Manually Registering and Deregistering the DMZ Gateway Daemon (non-Windows Systems) 2258

RedHat Enterprise Linux 2258
SuSE Linux 2258
Ubuntu Linux 2259
Solaris 2259
Uninstalling DMZ Gateway 2261
Uninstalling DMZ Gateway on a Windows System 2261
Uninstalling DMZ Gateway on a non-Windows System 2261
RedHat Enterprise Linux, SuSE Linux, or Solaris x86 32-Bit or 64-Bit 2261
Ubuntu Linux 32-Bit or 64-Bit 2261
Example of Uninstallation Process on Solaris 2262
Upgrading or Repairing DMZ Gateway 2263
Interface Reference 2265
The DMZ Gateway Interface 2266
DMZ Gateway Administration Interface PID File 2266
IP Access Exception Entry Dialog Box 2268
New Profile Wizard--Profile name 2269
New Profile Wizard--Peer Server Access 2270
New Profile Wizard--Configuration 2271
Frequently Used Non-Windows Commands 2272
Administering DMZ Gateway 2275
Initialization and Connection Diagrams 2276
Frequently Used Non-Windows Commands 2280
Controlling Access by IP Address 2283

Default Network Ports for EFT and DMZ Gateway 2284
Creating a DMZ Gateway Profile 2287
Deleting a Profile 2289
Editing a Profile 2290
Renaming a Profile 2291
DMZ Gateway Components 2292
DMZ Gateway Server 2292
DMZ Gateway Server Service 2292
DMZ Gateway Administration Interface 2292
DMZ Gateway System Files 2293
DMZ Gateway Headless Administration 2294
X11 Server Method 2294
Manual Configuration Method 2294
DMZ Gateway Logging 2296
DMZ Gateway Communications Activity Logging 2296
DMZ Gateway Server Diagnostics Logging 2297
Appenders 2298
DMZ Gateway Server Service Diagnostics Logging 2298
DMZ Gateway Statistics Logging 2298
DMZ Gateway Server Event Viewer (Windows Operating Systems Only) 2299
DMZ Gateway Server Syslog (Solaris/Linux-based Operating Systems Only) 2300
DMZ Gateway Administration Interface Logging 2300
DMZ Gateway Administration Diagnostics Logging 2300

DMZ Gateway Administrator Launcher Diagnostics Logging 2301
DMZ Gateway Server Configuration File (gwconfig.xml) Reference 2302
Configuration Validation 2302
Configuration Elements 2302
File Location 2307
Shared Configuration Location 2307
DMZ Gateway Server Unix/Solaris Daemon 2309
DMZ Gateway Status 2310
Routing AS2 Traffic through DMZ Gateway 2312
Specifying the Listening IP Addresses 2313
What Does This Mean for the Peer Server Listeners? 2314
What Does This Mean for the Client Listeners? 2315
Starting and Stopping the DMZ Gateway Server Service 2316
DMZ Gateway Server PID Files 2317
DMZ Gateway Server Status Files 2317
DMZ Gateway Server Monitoring 2317
Testing the Configuration 2318
Troubleshooting DMZ Gateway Communication 2319
Using DMZ Gateway as an Outbound Proxy 2321
Viewing Statistics 2322
Peer Notification Channels Tab 2322
Client Listeners Tab 2323
Statistics Tab 2324

DMZ Gateway Secure PNC 2325
Introduction to Secure PNC 2326
Configuring Secure PNC 2327
Configuring Secure PNC using a Self-Signed Certificate 2327
Configuring Secure PNC using an EFT Certificate 2327
Secure PNC Settings 2332
Secure PNC Logging 2336
The EFT REST API 2337
What is REST API? 2338
Enabling REST API for Remote Administration 2340
REST API Support via DMZ Gateway 2342
Configuring REST Permission Roles 2343
Using REST API for Connection Profiles 2365
Using REST API for Upload Quotas 2368
Using REST API to Retrieve Server and Site Metrics 2371
Using REST API to Authenticate REST-Authorized Administrators 2373
Server REST API 2376
Endpoint: /server 2377
Endpoint:/server/status 2380
Endpoint: /server/metrics 2382
Endpoint: /server/security/tls 2384
Endpoint: /server/security/ssh 2388
Endpoint: /server/reports 2391

Endpoint: /server/admin-users 2394
Endpoint: /server/admin-users/{adminId} 2398
Endpoint: /server/admin-users-policy 2402
Endpoint: /experimental/server/templates/{templateName} 2406
Endpoint: /server/ha/upgrade 2409
Nodes REST API 2411
Endpoint: /nodes 2412
Endpoint: /nodes/{nodeId}/metrics 2414
Endpoint: /nodes/{nodeId}/licenses 2416
Endpoint: /nodes/{nodeId}/licenses/{moduleName} 2420
Endpoint: /nodes/{nodeId}/licenses/trial-extension-challenge 2422
Endpoint: /nodes/{nodeId}/licenses/trial-extension-response 2424
Site Endpoints 2425
Endpoint: /sites 2427
Endpoint:/sites/status 2430
Endpoint: /sites/{siteId} 2432
Endpoint: /sites/{siteId}/metrics 2434
Endpoint: /sites/{siteId}/authentication 2436
Endpoint: /sites/{siteId}/general 2442
Endpoint: /sites/{siteID}/ftps 2446
Endpoint: /sites/{siteId}/https 2451
Endpoint: /sites/{siteId}/networkAndSecurity 2456
Endpoint: /sites/{siteId}/ipAccess 2461

Endpoint: /sites/{siteId}/ipAccessList/{ipAccessId} 2465

Endpoint: /sites/{siteId}/ipAutoBanList 2469

Endpoint: /sites/{siteId}/ipAutoBanList/{ipAutoBanId} 2470

Endpoint: /sites/{siteId}/sms 2472

Endpoint: /sites/{siteId}/sms/{profileName} 2477

Endpoint: /sites/{siteId}/accountSecurity 2484

Endpoint: /sites/{ siteId}/workspaces 2491

Endpoint: /sites/{siteId}/sendPortal 2494

Endpoint: /sites/{ siteId}/dropOffPortal 2499

Endpoint: /sites/{siteId}/privacyPolicy 2504

Endpoint: /sites/{siteId}/termsOfService 2507

Endpoint: /sites/{siteId}/gdpr 2510

Endpoint: /sites/{siteId}/uploadForms 2516

Endpoint: /sites/{siteId}/uploadForms/{uploadFormName} 2519

Endpoint: /sites/{siteId}/outlookDeploymentScript 2524

Endpoint: /sites/{siteId}/contentIntegrity 2525

Endpoint: /sites/{siteId}/contentIntegrity/{profileId} 2530

Endpoint: /sites/{siteId}/custom-commands 2537

Endpoint: /sites/{siteId}/custom-commands/{customCommandID} 2541

Endpoint: /sites/{siteId}/user-templates 2548

Endpoint: /sites/{siteId}/user-templates/{userTemplateid} 2554

Endpoint: /sites/{siteId}/user-groups 2562

Endpoint: /sites/{siteId}/user-groups/{groupid} 2565

Endpoint: /sites/{siteId}/user-groups/{groupid}/relationships/users 2570
Endpoint: /sites/{siteId}/ram/agents 2575
Endpoint: /sites/{siteId}/ram/agents/{remoteAgentID} 2578
Endpoint: /sites/{siteId}/ram/agents/templates 2580
Endpoint: /sites/{siteId}/ram/agents/templates/{remoteAgentsTemplateID} 2585
Endpoint:/sites/{siteId}/awe-tasks 2590
Endpoint:/sites/{siteId}/awe-tasks/{aweTaskID} 2594
Endpoint:/sites/{siteId}/awe-tasks-folders 2599
Endpoint:/sites/{sitetId}/awe-tasks-folders/{aweTaskFolderID} 2603
Endpoint: /sites/{siteId}/connection-profiles 2608
Endpoint: /sites/{siteId}/connection-profiles/{connectionProfileID} 2613
Endpoint: /experimental/site/templates/{templateName} 2618
Endpoint:/sites/{siteID}/dmz 2621
Security REST API 2625
Endpoint: /lists/security/ssh/algorithms 2626
Endpoint: /lists/security/tls/algorithms 2627
Endpoint: /lists/security/tls/ciphers/{cipherString} 2629
Login/Logout REST API 2631
Endpoint: /logout 2631
Keep-Alive REST API 2632
Endpoint: /keep-alive 2632
Users REST API 2633
Endpoint: /sites/{siteId}/users 2634

Endpoint: /sites/{siteid}/users/{userid} 2650

Endpoint: /rpc/sites/{siteid}/users/{userid} 2655

Endpoint: /sites/{siteid}/users/{userid}/as2inbound 2657

Endpoint: /sites/{siteid}/users/{userid}/as2outbound 2661

Endpoint: /sites/{siteid}/users/{userid}/counters 2664

Filesystem REST API 2666

Endpoint: /sites/{siteId}/filesystem/folders 2667

Endpoint: /sites/{siteId}/filesystem/folders/{folderid} 2669

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/folders 2677

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/permissions 2679

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/permissions/{folderpermid} 2684

Event Rules REST API 2689

Endpoint: /sites/{siteid}/event-rules 2690

Endpoint: /sites/{siteid}/event-rules/{ruleid} 2708

Endpoint: /sites/{siteid}/event-rule-folders 2710

Endpoint: /sites/{siteid}/event-rule-folders/{folderid} 2713

EFT REST API Reference (PDF) 2717

EFT COM API 2933

Business Activity Monitoring (BAM) 2934

Getting Support 2935

Server License Information 2935

Generate Support Data 2935

Using the Knowledgebase 2939

Support Home 2939

Introduction to EFT Managed File Transfer

More than just a managed file transfer (MFT) solution, Globalscape's Enhanced File Transfer (EFT) extends beyond standard MFT to allow you to connect with any industry-standard file-transfer client. With powerful security for meeting business and regulatory requirements, EFT ensures that encrypted transactions occur only with the appropriate entities, and that data confidentiality and integrity are preserved during transport and storage. EFT modular form makes it affordable by allowing you to purchase just the functionality you need, and add advanced features as your business needs change. That is, all module features are available during the trial.

EFT managed file transfer is available for the large enterprise and for small-to-medium businesses EFT Arcus is our cloud implementation. You can also deploy EFT in a hybrid environment (both on premises and in the cloud), and deploy EFT on an Amazon EC2 instance (virtual server in the cloud).

Refer to the Feature Availability table to view features available in EFT.

> **NOTE:** The Auditing and Reporting Module (ARM), is required to generate reports of data from the modules listed below. Refer to Descriptions_of_Preconfigured_Reports.htm for details.

Available Modules (licenses required)

- **Advanced Authentication Modes Module (AAMM)** - The Advanced Authentication Modes Module protects data in transit by enforcing the use of secure protocols, strong ciphers and encryption keys, and maintaining strict password policies, and enables organizations to centralize their user access controls, improve productivity, and increase adherence to security policies, and provides administrators with the ability to easily maintain password security in one location to quickly commission and decommission user provisions in one central location. The module also provides SAML (WebSSO), RSA SecurID, RADIUS, and CAC support, which allows EFT to fit in seamlessly with existing authentication measures.
- **Advanced Workflow Module (AWM)** - Formerly the "Advanced Workflow Engine" (AWE), the Advanced Workflow module adds additional automation capabilities, allowing you to add scripting and variables to *Workflow Tasks*, then add these reusable Workflows to Event Rules. A Workflow is a series of steps that can perform file transfers, batch data processing, application testing, and so on, and are defined to run automatically when started by some

event.

- **AS2 Protocol Module (AS2)** - Supports the exchange of structured business data securely on top of the HTTP or HTTP/S protocol. The Auditing and Reporting module must be installed. (The ARM trial is installed when you install EFT.)
- **Auditing and Reporting Module (ARM)** - Captures all of the transactions passing through EFT. You can query the data and create/view reports from within the EFT administration interface.
- **DMZ Gateway®** - used in combination with EFT to create a multitier security solution for data storage and retrieval. The DMZ Gateway resides at the edge of the network, brokering data between EFT residing behind your corporate firewall and your clients in the outside world.
- **Cloud Connector Module (CCM)** - Enables you to transfer files to and from cloud services such as AWS and Azure.
- **Enterprise Actions Module (EAM)** - Enables automation features (event rules) such as executing scripts, performing folder and file operations, compressing and decompressing files, and so on.
- **File Transfer Client (FTC)** - Enables you to define copy, move, and download actions in Event Rules. For example, you could define a rule to trigger when a file is downloaded, so that EFT moves it to another folder.
- **Folder Monitor Module (FMM)** - Creates an Event Rule trigger used to detect the creation, deletion, and renaming of files in a monitored folder and to perform Actions based on these triggers. For example, perhaps a weekly report is uploaded to a specific folder. You can define an Event Rule so that when EFT detects that a file has been added to the folder, an email is sent to notify one or more users that the report is available for download. As of v8.0.7, the FMM is no longer part of core EFT and requires a license to use the Upload, Download, Synchronize actions in event rules.
- **FTPS module** - Allows you to use FTP over SSL/TLS to for more secure transfers. (Plain FTP is included.)
- **HTTPS module** - Allows you to set up a secure connection to anyone in minutes using any Web browser. The HTTPS module adds the HTTP and HTTPS protocols to EFT, enabling you to support browser-based transfers without having to install a Web server. HTTPS encrypts the session data using the SSL (Secure Socket Layer) protocol, which provides protection from eavesdroppers and man-in-the-middle attacks. The Web Transfer Client (WTC) can deploy automatically upon client connection to EFT and can be used by any trading partner using virtually any Web browser.

- **Mobile Transfer Client** The Globalscape MTC v1 is designed to work exclusively with Globalscape's managed file transfer solution known as EFT. With the Globalscape MTC, organizations can provide employees, partners, and customers with access to corporate data from their mobile devices, while keeping the data safe and secure within the organizational boundaries.
- **OpenPGP module (PGP)** - Safeguards data at rest. The OpenPGP data encryption or decryption process is directed by Event Rules that specify how data files are treated in a particular context. EFT uses OpenPGP to encrypt uploaded data and the off-load capabilities of EFT to move the file to another location. (industry-standard, RFC 4880compliant)
- **Regulatory Compliance Module (RCM)** - Supports PCI DSS, GDPR, and other compliance-related features to achieve or exceed security practices mandated by government and industry standards such as PCI DSS, HIPAA, and Sarbanes-Oxley for data transfer, access, and storage.
- **Remote Agent module (RAM)** - Provides centralized control for automating transactions from distributed systems. RAM enables automatic interactions between branch offices, point-of-sale terminals, business partners, field agent laptops, or other remote systems and your EFT server (over HTTPS port 443) residing in a central location.
- **Secure Forms Module (SFM)** - Provides "upload forms," custom web forms that you create to capture metadata during file uploads when using the web clients. Metadata gathered by the upload form can be used in downstream event rules (that is, subsequent Actions) for conditional post processing.
- **SFTP Module** - Subset of the popular SSH protocol and is a platform independent, secure transfer protocol. SFTP provides a single connection port for easy firewall navigation, password and public key authentication, and strong data encryption, to prevent login, data, and session information from being intercepted and/or modified in transit.
  The SFTP module enables EFT to authenticate and transfer data securely with SFTP-ready FTP clients, such as CuteFTP®.
- **Timer Event Module (TEM)** - Allows you to execute a specified Action only one time or repeatedly at specified intervals. For example, you could schedule an Action (for example, generate and send a report) to occur on July 8 at midnight, or every Monday morning, or on the last Friday of every month at 2 a.m.
- **Workspaces**- Allows you to share folders and their files with internal and external users.

Additional tools (license required):

- Business Activity Monitoring (BAM) is a web-based dashboard tool that uses data from the Auditing and Reporting module to provide full visibility into the

flow of data through your EFT system. Evaluate data trends over time and gain instantaneous knowledge about the current state of your system.

What's New in EFT?

Below is a **high-level summary** of changes in each recent versions of EFT, with links to relevant help topics. **For a detailed log** of changes and fixes, refer to the release notes in the Client Success Portal.

> **NOTE:** If you don't have an account for the Client Success Portal, create an account using the name, email address, and serial number registered for your purchase.

v8.3.0

New Features

Administration

- Added ability to disable an administrator user after a period of inactivity.
- Added MFA to the EFT administrator accounts (PCI DSS 8.4.2).
- Increased EFT Admin password length; Passwords can be a minimum of 12 characters, but default to 15 characters to meet regulatory compliance standards. (PCI DSS 8.3.6).
- Added the ability to configure the App Data directory in the EFT installer.
- Added changes to folder encryption, data at rest.

ARM

- Updated OLE SQL Driver in EFT.
- Added new tables to ARM schema: **tbl_Actions** and **tbl_ClientOperations**. Refer to Knowledgebase article #11031 for details of ARM schema changes.

Advanced Workflow Module

- Advanced property `GSAWEMaximumQueuedTasks` was missing the second *m*and has been corrected. Be sure to update your advancedproperties.json file if you use this AP in v8.3 and later.

High Availability

- Changed default MSMQ to Unicast (msmq-iterative) (Advanced Properties "ClusterCoherenceQueueMsmqType").
    - Applies only to new installations. Upon upgrade, EFT will honor the previously configured value.

PGP

- Updated PGP library to 2024.

REST API

- Added REST API support to DMZ Gateway.

Web Admin Client (WAC), WTC, & Workspaces

- Added ability to set default expiration option for portals
- Added text displaying Workspace expiration in WTC
- Added support for Content Security Policy level-3 "strict-dynamic" to mitigate cross-site scripting (Refer to Knowlegebase article 11435 - Specify CSP).
- Added the ability to identify EFT's Site authentication

Enhancements

- Updated OpenSSL library to v 3.4.1 for Non-FIPS.
- Updated OpenSSH library to v9.8.
- Updated Generate Support Data to include EFT's Advanced Properties json file.
- Updated compression library.
- Updated the EFT installer to include SQL Express 2022.
- Updated Automate to v24.2.50.1.

Administration

- Added ability to disable an admin user after a period of inactivity.
- Updated administrator password security-policy defaults, such as enable anti-DOS feature, complex passwords, password history setting (PCI DSS 8.3.7), password expiration.
- Updated User Password Security defaults.
- Updated EFT logger file to enable log4cplus.rootLogger=INFO (syslog).
- Updated Azure Storage Client library.
- Updated the registration status of subscription keys in **Help > About** based on the invoice end date for new activations.
- Enabled Expire passwords for administrators by default (PCI DSS 8.3.10.1).
    - Applies only to new installations. Upon upgrade, EFT will honor the previously configured value.

- Added support for Subscription licensing registration via our Manual Registration process.
- Added a new column under the Transfers as Client in the UI to include EFT Event Rule names.
- Removed the bundled help file (chm) for EFT; help now requires internet access.

ARM

- Updated OLE SQL Driver in EFT.

Web Admin, WTC, & Workspaces

- Updated WTC Content Security Policy (CSP) Level 3 'strict-dynamic' to mitigate cross-site scripting.
- Updated Angular to v19.
- Updated anti-CSRF in EFT based on OWASP’s best practices.
- Replaced Brandon Grotesque font with Google’s Roboto.

Feature Availability

> **NOTE:** Please refer to the topic EFT Arcus Features in the Globalscape Knowledgebase if you are comparing EFT on-premises to EFT Arcus.

The tables below describe which features are included in EFT on premises, and which are available with the licensing of the modules.

Core Features of EFT

These features are part of EFT, but you still need to activate an EFT license after the trial has ended. Use of certain core features will require an additional module (such as HTTP/S, SFTP, or FTPS) or external tools (such as connection to an LDAP or ICAP server). Refer to the feature tables under Features by Category for details.

Active-Active clustering (HA)
Active-passive clustering (Failover for high availability)
Administrative console
Admin roles and permissions
Audit performance counters to Windows Perfmon
Auditing to text file
Auditing internal metrics to local database
Backup and restore wizard
Ban file types by extension
Batch management of users
Built-in, NTLM, AD, and LDAP auth (including AD admin auth)
COM API
Connection Profiles (requires HTTP/S, SFTP, or FTPS to connect as the server)
Content Integrity Control (CIC)
Delegated administration
Denial of server and flood protection
Else conditional logic in rules
Encrypted folders (secure data at rest)
Expire inactive accounts (including admin accounts)
Expire passwords after N days (including admin accounts)
Expiration reminder
FIPS 140-2-certified crypto (requires SSL/TLS or SFTP)

FTP plain (FTPS requires FTPS module)
IP white/black listing
Mobile file transfer
Override VFS credentials
Password complexity
Performance counters
REST-based administration
Reusable connection profiles
Run command-line scripts
SSL client cert auth (full functionality available only when HTTP/S or FTPs module is registered)
Triggers based on incoming (uploaded) files
Virtual folders mapped to shares
Windows EFS encryption
Event Rule Actions: • File scan for DLP/AV, ICAP/CIC • Flow: Stop Processing • Flow: Variable • Protocol: Email • System: Backup • System: Cleanup • User: Action • Windows: Event Log
Event Rules: • "IF" conditional for triggers • Create a change log for rules • "Else" conditional for triggers • Event Rule import/export • Group triggers into folders (Event Rule Folders) • Securable objects (Event Rule Permissions) • Connection Events (all) • File Server Events (all) • Server Events (all) • Site Events (all) • User Events (all)

Features by Category

These acronyms for the modules are used in the tables below:

AAMM = Advanced Authentication Modes Module

ARM = Auditing and Reporting Module

AS2 = AS2 protocol module

AWM = Automate Workflow Module

BAM = Business Activity Monitoring

CCM = Cloud Connector Module

DMZ = DMZ Gateway

EAM = Enterprise Actions Module

FMM = Folder Monitor Module

FTC = File Transfer Client

FTPS = FTPS module

HTTP/S = HTTP/S module

PGP = PGP Module

RAM = Remote Agent Module

RCM = Regulatory Compliance Module

SFM = Secure Forms Module

SFTP = SFTP module

TEM = Timer Event Module

WSM = Workspaces

Protocols

Feature	Core or module
FTP protocol (RFC 959)	Core
FTP extensions (multi-part, resume, parallel threads, file integrity checking, custom commands, S-Key, PASV port range, UTF-8, customizable banner, command blocking, EBCDIC mode, PASV port range controls)	Core
SSL/TLS 1.2 – for secure communications	Core
SSL certificate management	Core
SSL client certificate authentication	Core
SSL control over ciphers, algorithms, and protocols	Core
Real-time session monitoring	Core
SFTP protocol	SFTP
SFTP advanced options (multiple auth methods)	SFTP
SFTP key management	SFTP
SFTP control over ciphers, algorithms, and protocols	SFTP
FIPS 140-2 certified cryptographic module (Requires SFTP or HTTP/S to function properly)	Core

Feature	Core or module
HTTP/S protocol	HTTP/S
HTTP/S extensions (various auths including IWA/SSO, configurable headers, compliance with OWASP security guidelines, HSTS support, many other headers,)	HTTP/S
Web client – Built-in web client adds a rich set of features compared to script-driven HTTP/S transfers	HTTP/S
HTTP to HTTP/S auto-redirect	HTTP/S
Customizable HTTP error messages	HTTP/S
Mobile access via native mobile transfer client) – For iOS and Android	HTTP/S
AS2 protocol	HTTP/S & AS2 module
AS2 extensions (Message Level Security (MLS), Reliability Profile, Multiple Attachments (MA) profile.	HTTP/S & AS2 module

Authentication (Access Controls)

Feature	Core or module
EFT-managedaccounts (i.e., "built-in authentication, or Globalscape authentication)	Core
Active Directory (AD) – native Windows integration, including admin accounts) (In EFT Arcus, "AD impersonation" is available, but not authentication.)	Core
ODBC- leverage any ODBC data source	Core
LDAP- authenticate against LDAP sources, including AD	Core
SAML (WebSSO) - including Just In Time (JIT) provisioning	AAMM
RADIUS- often used as a two-factor authentication source	AAMM
RSA SecurID® (native and Steel-Belted Radius (SBR))	AAMM
CAC- Common Access Card authentication	AAMM
Secrets module	CCM
SMS authentication - two-factor authentication (2FA) for WTC and Workspaces	HTTP/S, WSM

Authorization (Resource Controls)

Feature	Core or module
AD Impersonation - Active Directory manages permissions	Core
AD-based administration accounts	Core
EFT managed folder permissions	Core

Feature	Core or module
Role-based administrator accounts with granular permissions (Delegated administration)	Core
Permission groups – templatize sets of permissions	Core
Virtual folders - map virtual to physical folders including network shares	Core
Home folders - designate a home folder and optionally make it the user's root folder	Core
Set limits - number of logins, connections, file sizes, transfer speeds, disk quotas	Core
DoS/flood detection algorithms and auto-IP ban logic	Core
IP access rules - full featured IP access rule manager (whitelisting/blacklisting)	Core
Ban file types by extension - prevent upload of unwanted file types	Core
Monitor and kick offending users from the server	Core
Invalid account names - controls to auto-ban offender IP	Core
Invalid passwords - controls to auto-lockout, disable, or ban IP	Core
Password complexity - configure a number of password complexity options	Core
Password reset - user-initiated or on initial login	Core
Password reuse - disallow historical (previously used) passwords	Core
Expire accounts - disable account on a given date	Core
Expire inactive accounts - disable or remove account after N days of inactivity	Core
Expire passwords - expire passwords after N days	Core
Expiration reminder - email user reminder to change their password	Core
Data sanitization - securely clean deleted data using military grade wiping	RCM
Encrypted folders - EFT built-in, secure-data-at-rest Solution	Core
EFS - encrypt data at rest using Windows' Streaming repository encryption (EFS)	Core
Override VFS credentials	Core
OpenPGP- use OpenPGP to encrypt, sign, and decrypt data	OpenPGP
PCI DSS- Site settings to facilitate PCI DSS and other compliance mandates	RCM
DMZ Gateway®- securely proxy transfers through the DMZ	DMZ Gateway®

Administration

Feature	Core or module
Silent installation - unattended setup	Core
Administrator GUI - Windows based Graphical User Interface (GUI)	Core
Remote administration - administrate from other systems in the network	Core
Secure remote administration - SSL encrypted administration communications	Core

Feature	Core or module
Multiple administrators - allow concurrent administration	Core
Secure administration - same password complexity options available for administrators as for users	Core
Flexible authentication - leverage native, NTLM, or AD to authenticate administrators	Core
Forensics- audit and report on all administrator activity and changes	ARM, RCM
COM API - programmatic administration	Core
REST endpoint for querying administrative info and server status	Core
Backup and Restore - one-click backup and easy restore of entire configuration **(Scheduled backups requires the TEM)**	Core
Batch account management - perform actions to multiple accounts simultaneously (such as multi-select users to reset their passwords)	Core
Specify personal data and privacy settings on a Site and per user	RCM
Generate GDPR DPIA report	ARM, RCM

Auditing and Visibility

Feature	Core or module
Logging - flat (text) file log in W3C and other formats	Core
Monitor transfers in real time	ARM
View historical transfers in the administration interface	ARM
Audit Performance counters to Windows Perfmon	Core
Audit internal metrics to local database	Core
Audit to SQL - audit transactions to a SQL database	ARM
View reports (predefined)	ARM
Create custom reports	ARM
Audit to Oracle - audit transactions to an Oracle database	ARM
Business Activity Monitoring (BAM) - real-time visibility, dashboard, and analytics (Requires ARM)	BAM, ARM

Automation (Integration with Other Systems)

Feature	Core or module
Event Rules change log	Core
Group Event Rules into folders	Core

Feature	Core or module
React to stimuli - trigger workflows based on file uploads and other server events	Core
Send email to users or administrators as part of a workflow	Core
"Stop processing if failed" action	Core
"If" and "Else" Conditions in Event Rules	Core
Connection Events	Core
Import/Export Event Rules	Core
Context variables - use transaction values inside of workflows	Core
Conditional logic - build fine-grained business logic into workflows	Core
Backup Action - Back up files **(Scheduled backups requires the TEM)**	Core
Cleanup Action - securely remove old files based on your organization's data retention policies **(Scheduled cleanup requires the TEM)**	Core
Upload and download- push or pull files to remote servers as part of a workflow	FTC
User Account Action - for tasks like re-enabling user accounts and compliance requests (for example, HIPAA, GDPR) in which users might ask that an organization remove all traces of their account.	Core
Windows Event Log Action	Core
Create reusable connection profiles for use in Event Rules	Core
Integration with antivirus and DLP (Data Loss Prevention) tools to permit or prevent transfers based on policies. **NOTE:** ◦ **Content Integrity Control** is used in event rules to send a file to an external antivirus scanner or data loss prevention solution for processing. ◦ Customer must install an antivirus/ data loss prevention solution. Any third-party content inspection product that supports ICAP can communicate with the Content Integrity Control in EFT. ◦ EFT Arcus has built-in Windows Defender antivirus protection at the OS level.	Core
File Server Events	Core
Server Events	Core
Site Events	Core
User Events	Core
Operating System Events	FMM, TEM

Feature	Core or module
Cloud-Based Events	CCM
Workspace Events	WSM, HTTP/S
Secure File Send Events	WSM, HTTP/S
AS2 Events	AS2
Subroutine Event	EAM
Send pre- and post- commands to mainframe during copy/move actions	FTC
Perform folderand fileoperations	EAM
Event Rule invoke over WS/SOAP (uses HTTP/S port)	EAM, HTTP/S
Web Services - trigger workflows using Web Service calls; Invoke Web Service from URL	CCM
Execute a process, including scripts, as part of a workflow	EAM
Folder monitor - trigger workflows immediately after files arrive in a monitored folder	FMM
Schedule events - trigger workflows on a recurring basis	TEM
Compress/Decompressfiles	EAM
Advanced workflows - tap into the Advanced Workflow module to build sophisticated workflows	AWM
Integration with cloud (AWS and Azure) storage; Copy, move, and download from cloud storage	CCM
Ability to monitor and act upon AWS S3 and Azure blob storage activity	CCM
Centralized control for automating transactions originating from distributed systems (Remote Agents), including provisioning, management and Event Rules	RAM
Run PowerShellscripts in Event Rules	EAM
Move tabular data between programs using the Protocol: listing to Dataset Action, Get/Loop from Host, and Import/Export to/from Dataset.	EAM

Person-to-Person (P2P) File Transfer

Feature	Core or module
Ad hoc file transfer – Allow authorized users to share files or folders with guest users via Outlookor using the EFT web interface, for secure P2P file exchange	HTTP/S, WSM
Two-way file sharing - recipients provided with multiple methods to securely send files to each other	HTTP/S, WSM
Receipt notification - email notification when files are picked up by the recipient	HTTP/S, WSM

Feature	Core or module
Pick-upauthentication - recipients can be required to verify their identity before downloading files	HTTP/S, WSM
Full file tracking - Users and administrators can view complete history of files sent and received	HTTP/S, WSM
Centralized policy controls - administrator can set defaults and mandate policies or let authorized users decide	HTTP/S, WSM
Mixed mode authentication - optionally authenticate internal employees against AD, while maintaining guest isolation	HTTP/S, WSM
Integration with EFT - monitor all ad hoc file transfer activity from EFT	HTTP/S, WSM
Request files – Authorized users can generate a request link that guests follow to securely upload files.	HTTP/S, WSM
Drop-off files to internal users with no attachment limits	HTTP/S, WSM
Manage personal data and privacy settings for GDPR and other privacy rules in the Workspaces client	HTTP/S, WSM, RCM
Multifactor authentication via email or SMS for client logins	HTTP/S, WSM
Gather metadata for uploads in the client via upload forms	HTTP/S, WSM, SFM
View sent and receivedmessages historyin client	HTTP/S, WSM

Architecture

Feature	Core or module
IPv6 - Full dual stack (IPv4/6 mixed) support	Core
Virtual - Install on virtual machines, e.g. VMware and Hyper-V	Core
Unicode - UTF-8 encoding of filenames and other fields where applicable	Core
IDN - Internationalized domain name support	Core
I/O Completion Ports - Technology that allows for fast performance on Windows systems	Core
Active-passive clustering - Failover for high availability	Core
Active-active, high availability (HA) clustering with two or more EFT servers	Core

Installing EFT and Modules

The instructions below describe how to install EFT.

1. Before You Begin - Information you should read before you start installation.
2. Installing or Upgrading - Information and procedures for installation and upgrading
3. After You Are Done - Information and procedures to follow after installing, such as configuring a connection and activating the software.

Before You Begin

When you first install EFT, wizards step you through creating a Server object, creating a Site (the connection to EFT), and creating your first user. Review the links at the list below to gain an understanding of what a typical EFT installation requires.

> **NOTE:** Even if you engage Globalscape Professional Services to deploy EFT in your network, there are steps that you need to follow prior to their engagement.

If you are installing EFT in the cloud, refer to the Globalscape Knowledgebase for information about EFT in AWS or Azure.

- For EFT on Amazon Web Services refer to: https://kb.globalscape.com/KnowledgebaseArticle11237.aspx
- For EFT on Microsoft Azure refer to: https://kb.globalscape.com/KnowledgebaseArticle11278.aspx

Before installation

- Review What's New? in your version of EFT
- Review the specifications, safe operating limits,and System Requirements for EFT and its modules
- If you are upgrading from a previous version, refer to Upgrading.
- Review EFT System Architecture
- Review Configuration and Security Best Practices
- If you're using DMZ Gateway:
  - Review how DMZ Gateway and EFT communicate
  - Review Default Network Ports for EFT and DMZ Gateway
- Review ARM storage requirements

System Requirements

Globalscape only offers support for EFT with the software and hardware on which we've tested EFT, as described below.

Listed below are the are the software applications that are compatible and supported on this version of EFT. (It is the customer's responsibility to install the correct versions.) For component versions that are packaged in EFT, refer to EFT Specifications.)

EFT (Server Service) Requirements

EFT and its modules can be installed on a physical computer, virtualization software such as VMWare, and in the cloud. EFT Arcus is our SaaS offering, hosted on Microsoft Azure.

- Operating systems:
  - Windows Server 2025
  - Windows Server 2022
  - Windows Server 2019
  - Windows 11 (administration interface only)
- Free RAM:
  - **Minimum**: 4 GB free RAM
  - **Recommended**: 8 GB free RAM (moderate Advanced Workflowsusage)
  - **High Performance**: 16 GB free RAM (if Advanced Workflowsare used extensively)
  - More RAM could be required for large file transfers over the AS2 protocol. AS2 transfers can use up to 40% of the Server's RAM.
- CPU:
  - **Minimum:**Dual-core CPU of at least 2.5GHz (for minimal processing/ automation)
  - **Recommended**: Quad-core, at least 2.5 GHz (for moderate processing/ automation)
  - **High Performance:**8+ cores, at 2.5 GHz (for high amount of processing/ automation)
- Microsoft .NET Framework 4.8 (.NET 4.8 is included in Windows Server 2022)
- EFT requires the following dependencies:

    - Microsoft ODBC Driver 17 for SQL Server (used for SQL ARM)
    - Microsoft OLE DB Driver v19.3.5 for SQL Server (used for SQL ARM)
    - Microsoft Visual Studio C++ 2010 x64 Redistributable – 10.0.30319
    - Microsoft Visual Studio C++ 2015-2022 Redistributable (x64) – 14.31.31103
    - Microsoft Visual Studio C++ 2015 -2022 Redistributable (x86) – 14.31.31103
- Max Latency (measured while not under load):
    - EFT to network share: <25ms
    - EFT to SQL/Oracle database: <10ms
    - EFT to DMZ Gateway: <50ms
    - EFT to Auth manager: <25ms
- **For HA (active-active) installations**:
    - Microsoft Message Queuing (MSMQ) must be installed.
    - Load balancer, such as F5®BIG-IP® Local Traffic Manager
    - File share (SMB or CIFS) for EFT configuration and users' files accessible via UNC path is required (configured as High Available storage for redundancy is recommended)

      NOTE:
      - DFS is not a supported platform for shared configuration. Refer to knowledgebase article #11569 Known Issues Using DFS on EFT for more information.
      - Azure Blob Storage is not a supported platform for shared configuration; may cause higher latency, requires additional configuration, lacks built-in file-locking mechanisms.

    - If file replication technology is used for Disaster Recovery, it must be configured as synchronous file replication. Technologies that use asynchronous file replication are not supported.
    - Fully qualified domain name (FQDN) or DNS record for File Shares and Databases is required and best practice
    - If *encryption at rest* is required, determine whether your storage vendor's solution includes built-in encryption or supports Microsoft's Encrypted File Shares (EFS). If neither option is available, you can leverage EFT built-in Encrypted Folders feature, which is available in standalone or high availability (HA) configurations.

    - Latency between all nodes should be the same. For example, if you have three nodes, A, B, and C, with latency between A and B at 50ms, but between A and C, or B and C is 100ms, this difference could cause EFT servers to crash, EFT server services restarts, configuration corruptions, and so on. Max Latency (measured while not under load):
    - EFT node to another EFT node: <25ms
    - Each EFT node to network share: <25ms, with no more than +/- 50% discrepancy between nodes (A single network share used both for EFT configuration and as a file repository. EFT does not support separate shares even if those are two-way synced.)
    - Each EFT node to shared SQL/Oracle database: <10ms, with no more than +/- 50% discrepancy between nodes
    - Each EFT to a DMZ Gateway: <50ms, with no more than +/- 50% discrepancy between nodes
    - Each EFT to shared Auth manager: <25ms, with no more than +/- 50% discrepancy between nodes
- If accessing or monitoring shares, SMB v2.0 or 3.0
- The EFT server service runs under a user account, which must have full administrative rights (permissions) to the folder in which you install EFT. With administrative rights, the service can save all of your settings. If the service does not have administrative rights, you will lose settings and user accounts whenever you restart the EFT service, and you will need to reset permissions on the computer on which the EFT service is running. If you are using Active Directory, there are other considerations regarding permissions.

EFT Administration Interface Requirements

The administration interface must be installed on the same computer as EFT, but also can be installed on other computers for remote administration. (Refer to the ARM, Advanced Workflows, and AS2 requirements below if you plan to use those modules remotely.)

- Windows Server 2022, 2025, 2019
- Windows 11
- 1 GB of free RAM
- 1280x1024 resolution or higher display
- Microsoft Windows Installer 4.5
- Microsoft .NET Framework 4.0 and later
- Microsoft .NET Framework 4.8 "Full"

Auditing and Reporting Module (ARM) Requirements

- Microsoft SQL Server drivers are installed automatically, regardless of whether SQL Server will be used. (You can read more about SQL Server drivers here: https://docs.microsoft.com/en-us/sql/connect/oledb/oledb-driver-for-sql-server?view=sql-server-2017.)
- 3GB minimum hard drive space for the initial database size. Space requirements for transactions depend on estimated Event Rule activity, number of connections, and types of transactions. A general estimate is 3MB to 5 MB per 1000 files uploaded.
- PDF-viewing software (such as Adobe Reader) to view PDF reports.
- Access to a SQL Server or an Oracle database.

  > **NOTE:** SQL Server Express 2022 is installed for testing purposes.

- EFT is supported with the following SQL Server version:
  - SQL Server 2022
  - SQL Server 2019
- Microsoft® ActiveX Data Objects (ADO)
  - EFT uses Microsoft ActiveX Data Objects (ADO) 2.7 or later to handle database communication, which in turn should load the Oracle drivers to handle Oracle implementation details. How and what is connected largely depends upon the connection string. By default (if you do not supply the entire connection string in EFT), the Oracle connection string should look like the example below. Replace the values in curly braces { } with the required values (host, port, database name, username, and password).

Oracle Connection String

```
Provider=OraOLEDB.Oracle.1;
 Data Source=(DESCRIPTION =
(ADDRESS_LIST = (ADDRESS
 = (PROTOCOL = TCP)(HOST = {host value})(PORT
 = {port})))"
(CONNECT_DATA =(SERVICE_NAME
 = {database name})));
Persist Security Info=true;PLSQLRSet=1;PwdChgDlg=0;User
 Id={username};Password={password};
```

- Refer to Oracle's documentation regarding Oracle system requirements. Be sure to reboot after you install the Oracle Data Access Components (ODAC). You must install both the 32-bit ODAC drivers for the report writer, and the 64-bit ODAC drivers for EFT to work with Oracle.
- EFT supports the following Oracle versions:
  - Oracle Database 19c

> **NOTE:** Older versions of SQL and/or Oracle could still work, however, they are no longer tested by the QA team.

- Don't use SQL Server Express Edition or Oracle Database Express Edition as the ARM production database.
- Install the ARM database on a separate database server; don't install EFT server and SQL Server Engine on the same operating system to avoid scaling issues during traffic peaks.
- Define and implement a database maintenance plan to keep space requirements to a minimum (aging/archiving/warehousing/truncating old data) that meets your business data retention requirements.
- For better database performance, follow the standard SQL/Oracle tuning guidelines in their respective documentation.
- For ARM upgrades, Microsoft .NET Framework 4.8

AS2 Module Requirements

- HTTP/S module
- AS2 module
- AS2 file transfers must not exceed 20GB.
- More RAM could be required for large, non-EDI file transfers. AS2 transfers can use up to 40% of the Server's RAM for file transfers.
- You must have .NET installed and configured. During installation, EFT determines whether .NET framework is installed and, if not installed, prompts you to install it.
- The Auditing and Reporting module (ARM) is not required, but is recommended for auditing purposes. (The receipt policy is not dependent on ARM.)

If the AS2 module is not activated (or no longer in trial mode):

- All incoming AS2 connections are rejected.
- EFT audits the failure in the ARM database as "AS2 evaluation license expired."

- Any Event Rule that contains the Protocol: AS2 action (AS2 Send File to host) will not fire; the If Failed Action triggers and ARM audits the outbound failure in the ARM database as "AS2 evaluation license expired."
- All AS2 configuration is "harcoded"/ not configurable (aside from your AS2 ID, SSL certificate, and AS2 portal page, configured on the **Site > Connections** tab).

Web Transfer Client (WTC) and Workspaces Requirements

The EFT installer is bundled with a compatible version of the WTC.

- 1280x800 resolution or higher display
- JavaScript must be enabled in the browser.
- WTC supports:
  - Directory listings that contain up to 1,000 items. More items can work on certain browsers; however 1,000 is the official (tested) supported item limit.
  - ASCII and UTF-8 encoded filenames that follow Windows' naming conventions
  - Directory trees up to the Windows "MAX_PATH" length, or 260 chars (note that this is absolute path, not relative path. Only the relative path is visible to the user).
- Web browser:
  - Unsupported browsers may force the use of the "plain-text client."
  - The WTC will work with most modern browsers that support HTML 5. Refer to https://kb.globalscape.com/KnowledgebaseArticle11367.aspxto see which browsers were tested with each version of EFT. (Internet Explorer does not support >4GB uploads.)
  - The browser running the client must have cookies enabled. Note that cookies work on IP addresses (for example, 127.0.0.0) or full domain names (for example, yourcompany.org), not *Localhost*.

Web Admin Client (WAC) Requirements

The EFT installer is bundled with a compatible version of the WAC.

- 1280x800 resolution or higher display
- JavaScript must be enabled in the browser.
- Web browser:

- The WAC will work with most modern browsers that support HTML 5. Refer to https://kb.globalscape.com/KnowledgebaseArticle11367.aspx to see which browsers were tested with each version of EFT.
- The browser running the client must have cookies enabled. Note that cookies work on IP addresses (for example, 127.0.0.0) or full domain names (for example, yourcompany.org), not Localhost.

Advanced Authentication Modes Module Requirements

- To generate PCI DSS reports, you will also need the Auditing and Reporting module.
- For Common Access Card authentication:
  - LDAP server
  - CAC smart card reader
  - EFT v8.x does not support UPLOADS from CAC-authenticated users when using Chrome or Edge browsers. Firefox (and possibly other browsers) will work.
- For RADIUSor RSA authentication:
  - RADIUS server
- For SAML (Web SSO) authentication:
  - Identity provider (for example, SafeNet, Salesforce, Shibboleth)

Regulatory Compliance Module (RCM) Requirements

- To generate PCI DSS and GDPR reports, you will also need the Auditing and Reporting module.

EFT Outlook Add-In Requirements

- The EFT Outlook Add-In is supported on Microsoft 365, Office 2019, with the latest service packs (as of this release).
- Microsoft .NET Framework 4.84.0
- Globalscape Support no longer tests the EFT Outlook Add-In with older versions, therefore it is not a supported configuration; however, some customers are still using those versions

DMZ Gateway® Requirements

- Refer to System Requirements for DMZ Gateway.
- EFT and DMZ Gateway cannot be installed on the same computer or virtual machine image, but must be installed no more than one network “hop” away with an average network latency no greater than 50ms, with zero percent packet loss, and normal packet flow. Refer to https://kb.globalscape.com/KnowledgebaseArticle11447.aspxfor more information.

Advanced Workflow Module Requirements

> **NOTE:** EFT v8.2.x includes some functionality of Automated Desktop 2024 as part of the Advanced Workflow Module. It is not backwards compatible with the Advanced Workflow Engine (Automate v10). It is not recommended to run a standalone Automate version with EFT. Only the bundled version of Automate has been verified to be fully compatible with EFT and no other version is officially supported.

- Advanced Workflows v10 requires Microsoft .NET Framework 4.0
- Advanced Workflows 2024 requires Microsoft .NET Framework 4.8. If you are installing on Microsoft Server 2022, .NET 4.8 is included and EFT v8.2.x will install without any prompts. On Microsoft Server 2019 or earlier, you will need to install .NET 4.8 ***before*** installing EFT v8.2.x.

Remote Agent Module (RAM) Requirements

- HTTP/HTTPS module
- SSL must enabled and available on port 443
- Visual C++ and Redistributable for Visual Studio (for installation)
- EFT server must be registered

- Operating systems supported: Windows Server 2025, Windows Server 2022, Windows Server 2019
- After installation, the computer may require a reboot

Mobile Transfer Client (MTC) System Requirements

MTC is supported on:

- Android- or iOS-based mobile devices of varying resolutions
- Android 2.3 or later for general operations
- Android 3.0 or later if encrypted data store is required
- iOS 6.1 or later (tested on both 6 and 7)

Content Integrity Control Action Requirements

The Content Integrity Control (CIC) Action requires a connection to an ICAP server. The CIC action was tested with:

- Clearswift (DLP) version 5_5_202211301821
- MyDLP Community Edition Server version 2.2.32-1
- Symantec DLP version 14.5.0.24028
- Kaspersky version 5.5

When using the CIC action, EFT needs to use POST in HTTP requests. Refer to Globalscape Knowledgebase article https://kb.globalscape.com/KnowledgebaseArticle11375.aspxfor information about enabling an advanced property.

EFT Specifications

This topic is intended as a quick reference of EFT specifications. Information is provided in detail in the applicable procedures.

See also:

- Safe Operating Limits for EFT
- EFT and Advanced Workflows Encryption Algorithms
- System Requirements

Item	Description
Protocols	• FTP/S (SSL/TLS), SFTP (SSH2), HTTP/S, and AS2 (Certain protocols other than FTP require optional modules.) • FTP Commands Supported by EFT • The FTPSprotocol in EFT is compliant with RFC4217, "Securing FTP with TLS." • EFT supports SFTP versions 2, 3, 4, and 6. The outbound client defaults to version 4, and it is not configurable through the GUI, but can be configured in advanced properties. The EFT outbound client negotiates the SFTP version with the receiving server during session establishment. That is, if the receiving server only supports version 2, EFT Server will negotiate down and operate at version 2. • SFTP hashing algorithmssupported: For both FIPS and non-FIPS ciphers and algorithms, refer to SFTP FIPS.

Item	Description
SSH version	• EFT v8.3.0 uses OpenSSH v9.8 • EFT v8.2.1 uses OpenSSH v9.5 • EFT v8.0.x and later use openssh library, including OpenSSH DLLs for FIPS. The EFT SFTP library implementation is based on the latest (8.1) version of OpenSSH portable: https://github.com/PowerShell/openssh-portable, which is a fork of https://github.com/openssh/openssh-portable, which in turn is a fork of the canonical OpenSSH. EFT will be updated once the fork that EFT is using is updated to 8.2, 8.3, or newer version. Also note that the EFT implementation contains some modified OpenSSH files, modified via use of a Fedora patch, for purposes of FIPS certification when FIPS mode is enabled.
SSL version (non-FIPS) Refer to "FIPS" below for the OpenSSL version used for FIPS.	• EFT v8.3.0 uses OpenSSL v3.4.1 (non-FIPS) • EFT v8.2.1 uses OpenSSL v3.1.4 (non-FIPS) • EFT v8.2.0.10 and later uses OpenSSL v3.1.4 (non-FIPS); In EFT v8.2.x, the SAML library was updated to OpenSSL v3.2.1. • EFT v8.1.0.16 uses OpenSSL v1.1.1t for SAML; everything else SSL related (except FIPS) uses OpenSSL v1.1.1o; • EFT v8.0.6 - 8.0.7 use OpenSSL v1.1.1k; • EFT v8.0.4 - 8.0.5 use OpenSSL v1.0.2u (dated December 20, 2019), SSL.dll and SSLfips.dll; • EFT v8.0.0 - v8.0.3 use OpenSSL v1.0.2t; TLSv1.2 is set by default. • For best security, in the TLS Settings dialog box, clear the check boxes for versions that you do not need enabled; do not enable SSLv3 cipher suites

Item	Description
FIPS	• EFT uses the FIPS Object Module; (In addition to the validations of the OpenSSL FIPS Object Module 2.0 obtained directly by OpenSSL, third-party vendors have obtained additional "re-brand" validations of the same cryptographic module.) • EFT v8.2.1and later use OpenSSL v3.1.4 for FIPS • OpenSSL v1.0.2u is FIPS-certified, but does not support TLS 1.3. EFT uses v1.0.2 for SFTP in FIPS and non-FIPS mode because SFTP doesn't care about TLS version • OpenSSL v1.1.1 has no FIPS module, but supports TLS 1.3; EFT uses it in non-FIPS mode to support TLS 1.3
SSL Certificate Key lengths supported	• Key lengths supported: 1024, 2048, 3072, and 4096 bits
EFT-created SSL certificates	• x.509 base-64 standard DER encoded
Allowed OpenSSL ciphers for inbound transfers (HTTPS and FTPS)	• Refer to the **Server > Security** tab for available ciphers.
Authentication types	• Built-in, AD/NTLM, LDAP, ODBC, RADIUS, RSA SecurID®
Log formats	• W3C, Microsoft IIS, and NCSA
OpenPGP	• EFT v8.3.0 uses IPWorks OpenPGP 2024 • EFT v8.10.5uses IPWorks OpenPGP 2020 v20.0.8136 from /n Software for secure OpenPGP messaging and advanced encryption and decryption and is RFC 4880 compliant.
PCI DSS	• EFT facilitates compliance with PCI DSS
AS2 module	• EFT uses /n software's EDI Integrator library components, which are in the core of an application called RSSBus. RSSBus is Drummond Certified and in compliance with RFC4130. (EFT itself is not Drummond certified.) The maximum inbound file size for AS2 transfers is 20GB; there is no limit on outbound file size.

Item	Description
Advanced Workflow Module (AWM)	• EFT v8.2 uses Automate Desktop 2024 Task Builder and actions • Visual Studio 2022
ICAP/ Content Integrity Control	• EFT supports RFC3507, sections 3.2 and 4.9. EFT supports: draft-stecher-icap-subid-00 section 4.5 and 4.6. • Microsoft .NET Framework 4.84.0 • Azure Storage C++ Client library v12
EFT Outlook Add-In library	• EFT v8.0.6 and later use Apache log4net v2.0.12
RSA library	• EFT 8.1 and later use RSA® Authentication Agent API 8.6
RegEx	• EFT uses the regular expression engine in .NET.
Web Clients	• EFT v8.3.x uses Angular v19 • EFT v8.2.1 uses Angular v17
WIX library	• EFT 8.2.1 uses Wix Toolset v4.0.5 (Used to create installers for Windows Installer.)
Azure Client Library (used in Connection Profiles with Azure Blob Storage and Azure Data Lake Storage)	• EFT 8.3.0 and later use the Azure SDK for C++ library • EFT 8.2.1 and earlier use the Azure Storage Client Library for C++.

Safe Operating Limits

The list of EFT object types and their maximum safe operating limits can be found at https://kb.globalscape.com/Knowledgebase/11543/Safe-Operating-Limits.

EFT System Architecture

EFT can be installed as a stand-alone deployment with one server (which can have multiple Sites/IP addresses). Several more complex options are available for how you configure EFT in your network architecture, described below, depending on what you need to accomplish.

Refer to the EFT System Architecture Guide in the Knowledgebase for descriptions and illustrations of the various architectures available.

Talk to your account manager or the Globalscape Professional Services team to design a custom architecture.

Installing EFT

The topics below provide information regarding installing and activating EFT, and configuring EFT on your network.

Before you run the installer, review the System Requirements, EFT Specifications, and the Knowledgebase article, Configuration and Best Practices.

- Installing the Server, Interface, and Modules
- Installing or Upgrading the Advanced Workflow Module
- Active-Active HA Cluster—Installing or Upgrading the Server
- Active-Passive Failover Clustering--Installing or Upgrading
- Upgrade HA Nodes with Zero Downtime
- Upgrading EFT
- Uninstalling the Software
- Silent Command-Line Installation
- Installation Logging

Installing EFT, Administration Interface, and Modules

The EFT installer is used to install EFT and its modules, except for DMZ Gateway.

Important Pre-Installation Information:

- **Before installing the software**, refer to System Requirements, and read the entire installation procedure below. Also review "Important information" in Installing the Advanced Workflow Module.
- After you have installed the system on a test computer and are now ready to move it to a production environment, refer to Backing Up or Restoring Server Configurationif you want to keep the test environment's Server, Site, and user configuration settings. Otherwise, perform a clean install as usual on the production system.
- **If you are installing in a cluster configuration**, refer to Installing or Upgrading the Server in a Cluster.
- **If you are connecting to an existing database**, ensure the database is installed and configured before starting the EFT installer. The installer will attempt to connect to the database. Or you can skip ARM installation and rerun the installer later in **Modify** mode.
- **If you are using an Oracle database**, ensure the ODAC client suitable for your database version is installed. (Refer to System Requirements.) For details of installing SQL Server, refer to the SQL Server Install pages on technet.microsoft.com.
- The EFT installer includes the ARM database installation and upgrade files. If you want to install or upgrade the database later, refer to Installing and Configuring the Auditing and Reporting Module, Upgrading the EFT Database, Upgrading Large Databases, and EFT Database Utility.
- The EFT installer does not support Unicode characters. Refer to Unicode Exceptions for details.

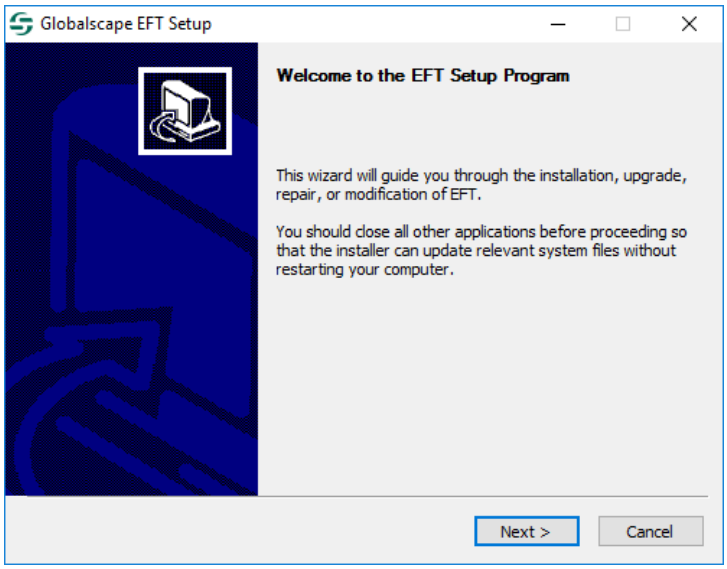
The installer verifies that the following items before continuing and will prompt you:

- OS compatibility
- Is the user an administrator?
- DMZ Gateway is ***not***installed on this server?
- Correct .NET version installed?

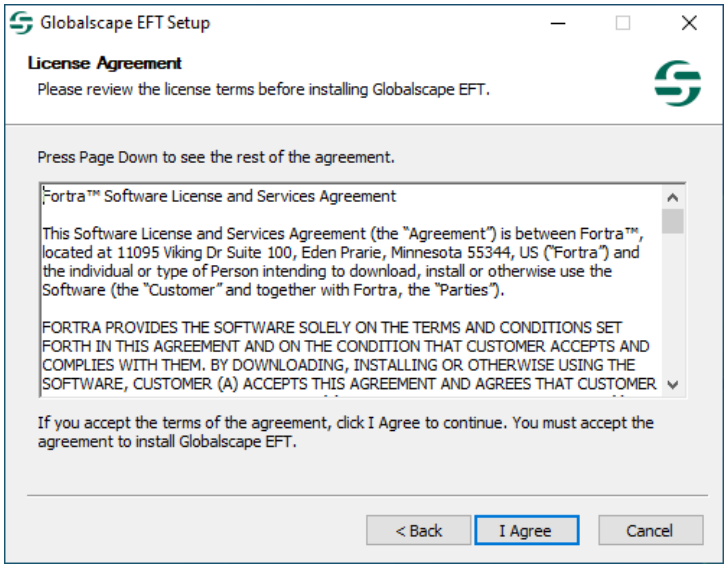
- MSI 4.5 installed?
- MSMQ installed? (HA installationsonly)

To install EFT, administration interface, and all modules except for DMZ Gateway

1. Close all unnecessary applications so that the installer can update system files without rebooting the computer.
2. Start the installer. The **Welcome** page appears.

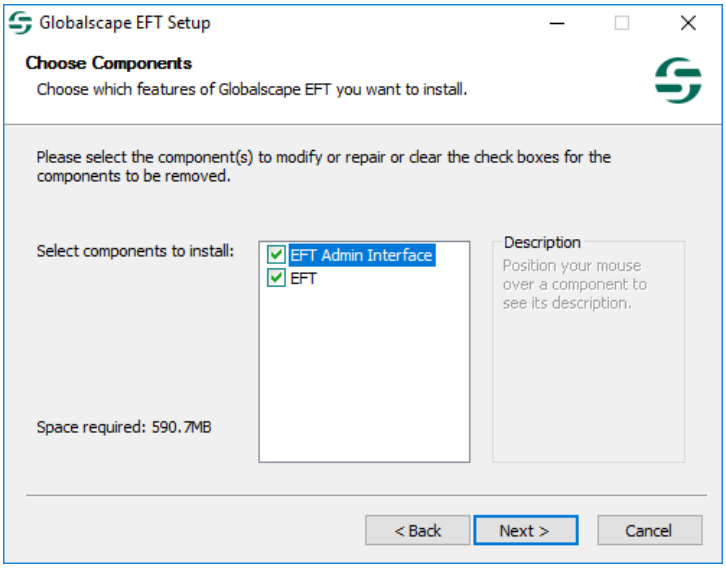


3. Read the **Welcome**page, and then click **Next**. The **License Agreement** page appears.



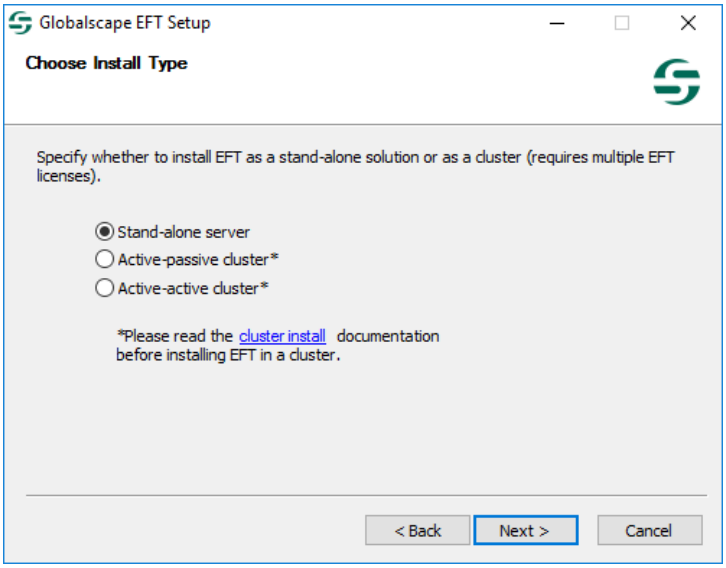
4. Read the license agreement, and then click **I agree** to accept it. Clicking **Cancel** aborts the installation.
    - If you are upgrading or reinstalling, the version detected page appears. Refer to Upgrading the Software for the procedure.

    The **Choose Components** page appears.



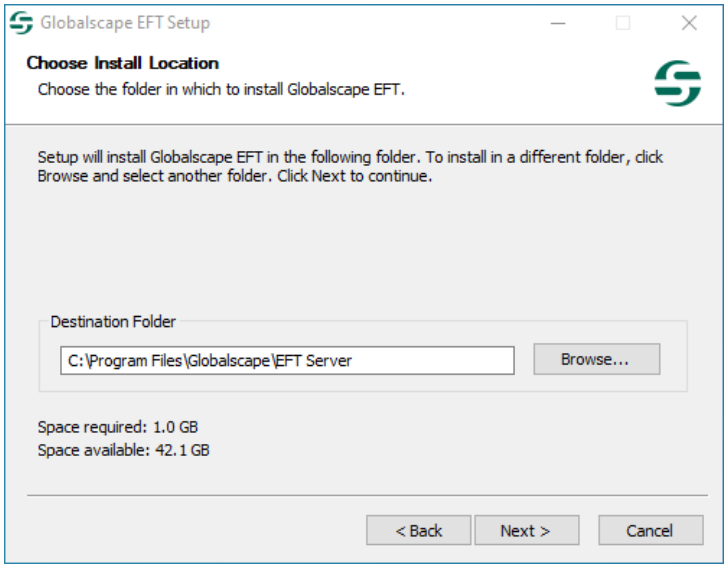
    When you install EFT, the **EFT administrator Interface** check box must also be selected. After you have installed EFT and the administration interface on one computer, you can install the administration interface on other computers for remote administration (optional). (To install the administration interface on a remote computer, refer to Installing the administration Interface Remotely.)

5. Click **Next**. The **Installation type** page appears.

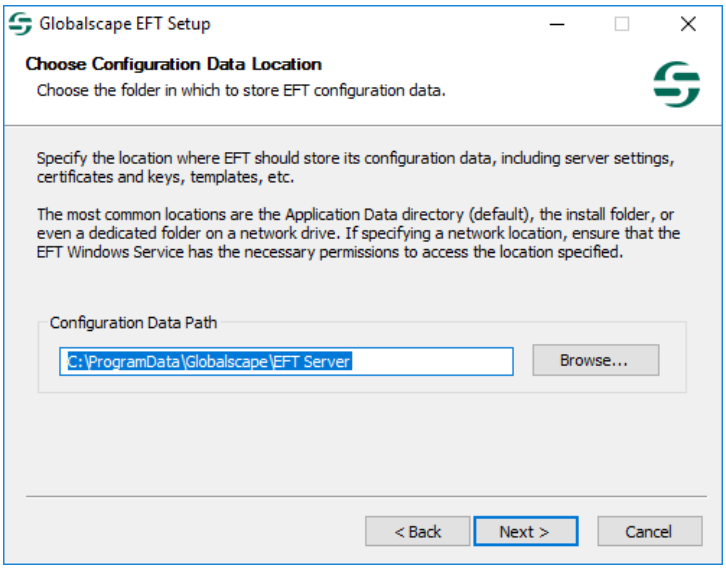


6. Specify the installation type, and then click **Next**.
    - Single server is the default installation type.
    - To install EFT as part of a failover cluster, review the cluster documentation, and then click **Part of a failover cluster**. A message appears cautioning that it is important to read and understand the cluster documentation if you are installing EFT in a cluster.
    - To install EFT as part of a high availability cluster, refer to Installing or Upgrading the Server in a Cluster.

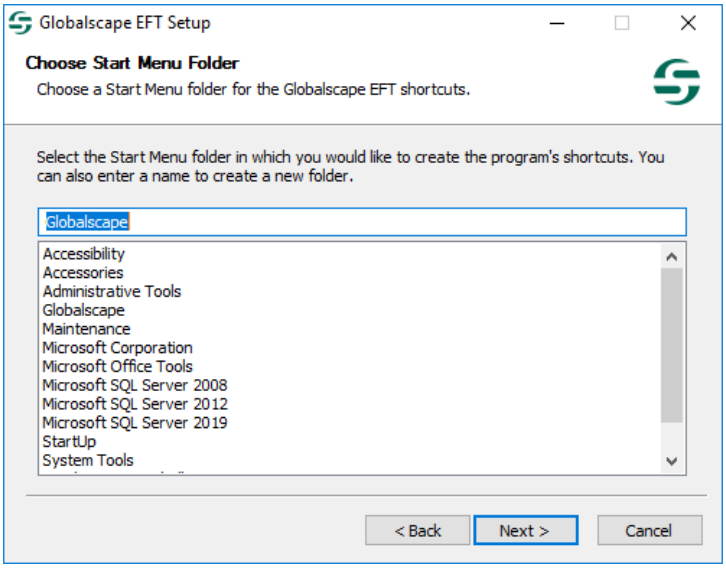
    The **Choose Install Location**page appears.



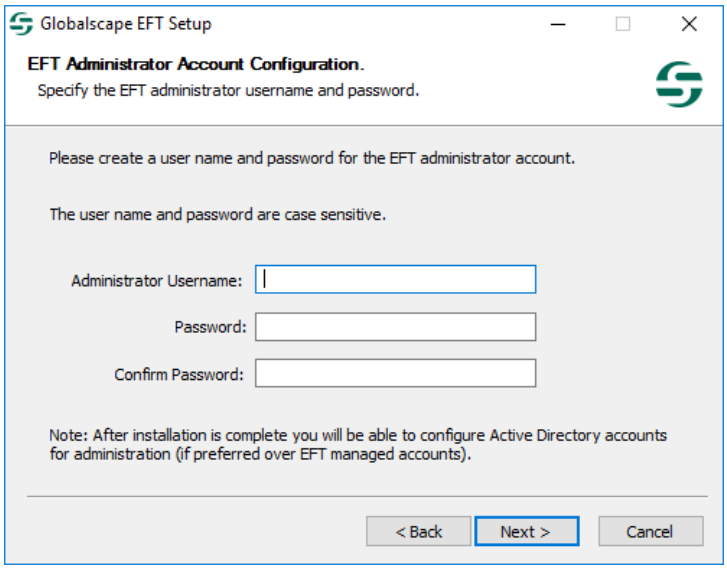
7. The default installation location appears in the **Destination Folder** box. Leave the default or click **Browse** to specify a different folder, and then click **Next**. The **Configuration Data Location**page appears. (The installer does not support Unicode characters in the path. Refer to Unicode Exceptions for details.)



8. Specify where you want to save the EFT configuration settings. For example, if you are installing in a cluster, you should specify a shared resource drive to synchronize settings across nodes. The EFT service must have permission to access the specified path. The default location is **%systemroot%\ProgramData**. The installer does not support Unicode characters in the path. (Refer to Unicode Exceptionsfor details.)
9. Click **Next**. The **Choose Start Menu Folder**page appears.



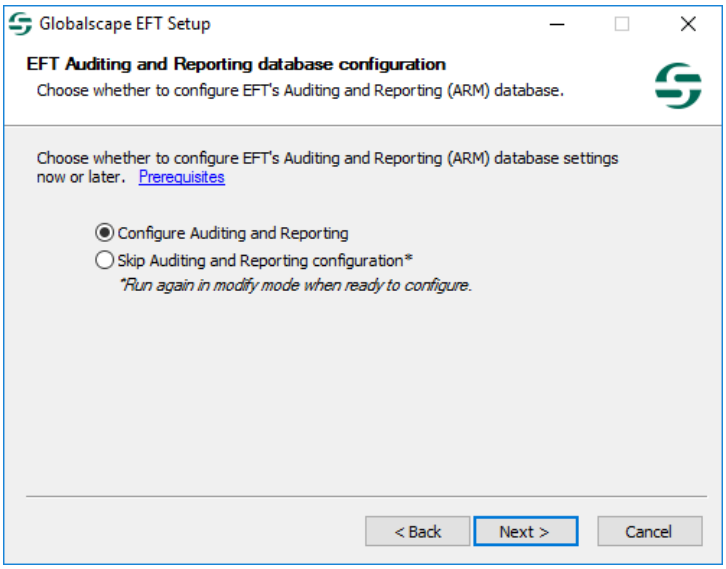
10. Keep the default shortcuts, specify an existing folder, or type a name for a new folder.
11. Click **Next**. The **Administrator Account Configuration**page appears.



12. Create a user name and password for the administrator account for connecting to EFT from the administration interface. Both the username and password are case sensitive. The installer does not support Unicode charactersin the username or password.

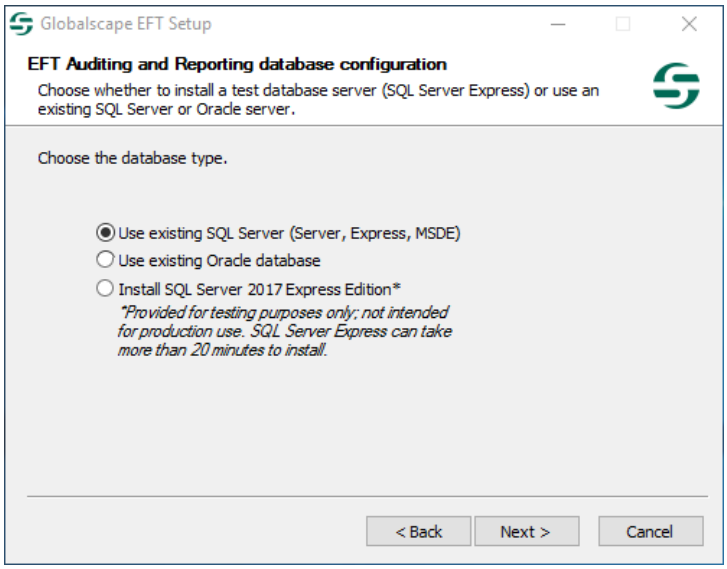
    > **NOTE:** The administrator account password cannot be blank, can be up to 99 characters, and cannot be any of the following keywords: `password`, `administrator`, `sa`, or `sysadmin`. The administrator account password must also comply with the computer's Windows account password policy (local or domain policy) "Minimum password length" and "Password must meet complexity" items. To view the policy, click **Start > Run**, then type `secpol.msc`. The **Local Security Policy**snap-in appears. Under **Security Settings**, expand **Account Policies**, and then click **Password Policy**. Right click the policy, and then click **Properties** to view the details and to enable, edit, or disable the policy.

13. Click **Next**. The ARM selection page appears.



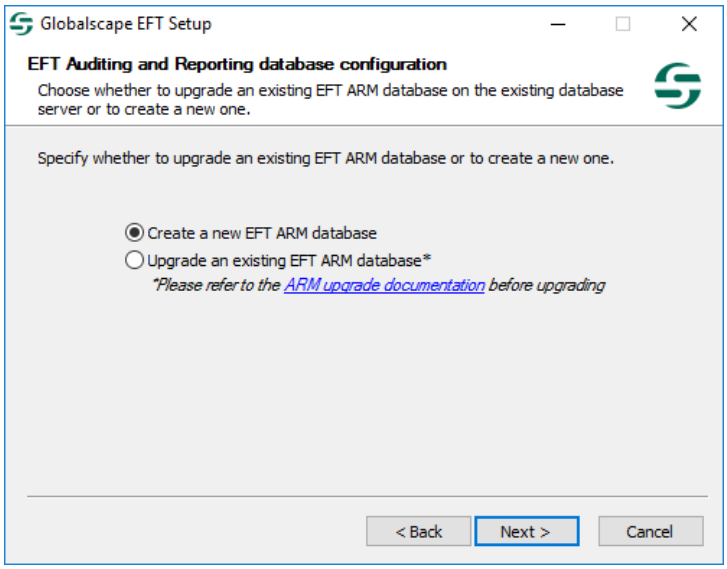
- If you want to configure auditing and reporting, click **Next**.
- If you do not want to configure auditing and reporting, click **Skip auditing and reporting configuration**, and then click **Next** to skip the database configuration pages. You can still configure the database later, if you want. (Skip to step 18.)
- If you want to manually create the database later, click **Skip auditing and reporting configuration**, and then refer to Manually Creating the ARM Database in SQL Server or Manually Creating the ARM Database in Oracle when you're ready to create the database. (Skip to step 18.)

14. Specify the type of database, SQL Server or Oracle, that EFT is to use. You will need the connection information available to point EFT to the database. If you already have a database to use, then you do not need to install SQL Server Express. (If you are using the "no db" installer, you will not see the "Install SQL Server" option.)

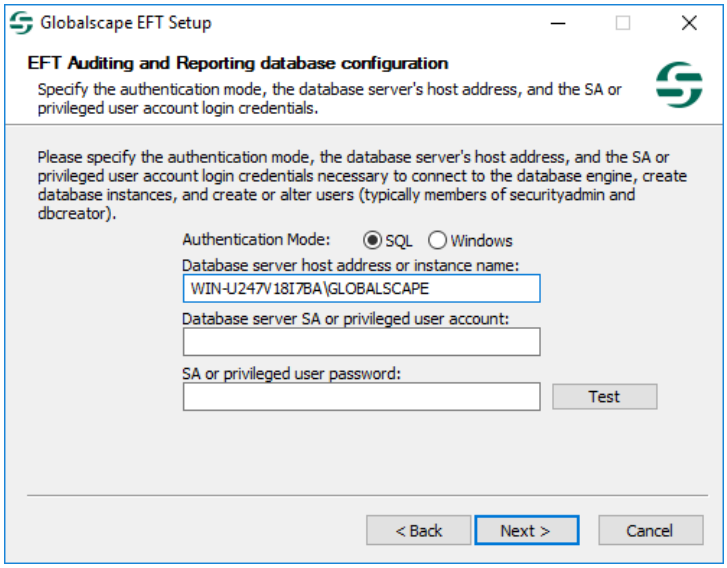


- **Install SQL Server Express**
  - SQL Server Express is provided for use in a trial. It is not intended for production use. During installation, a default system administrator account (the "sa" account) will be created within SQL Server Express. The EFT administrator account password will be used as the password for this "sa" account. Click **OK**to continue SQL Server Express installation and follow prompts to complete SQL Server Express installation.

- **Use existing SQL Server:**



a. Click **Create a new EFT ARM database**. The configuration page appears.



b. Specify **Windows**or **SQL** Authentication. (**Windows** mode allows you to connect through a Microsoft Windows NT or Windows 2000 user account. **SQL**allows you to connect using either Windows Authentication or SQL Server Authentication.)

c. Specify the host address or instance name.

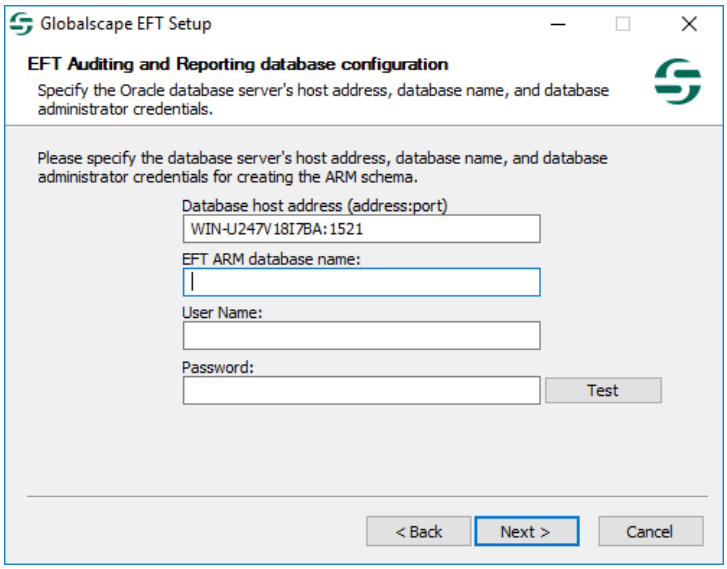
d. Specify the database server SA or privileged user account name (for example, sa).

e. Specify the database server SA or privileged user account password

f. (Optional) Click **Next**or **Test** to test the connection to the database. If the test fails, click **Yes** to verify database connection details or **No** to continue without configuring the database.

- **Use existing Oracle database:**

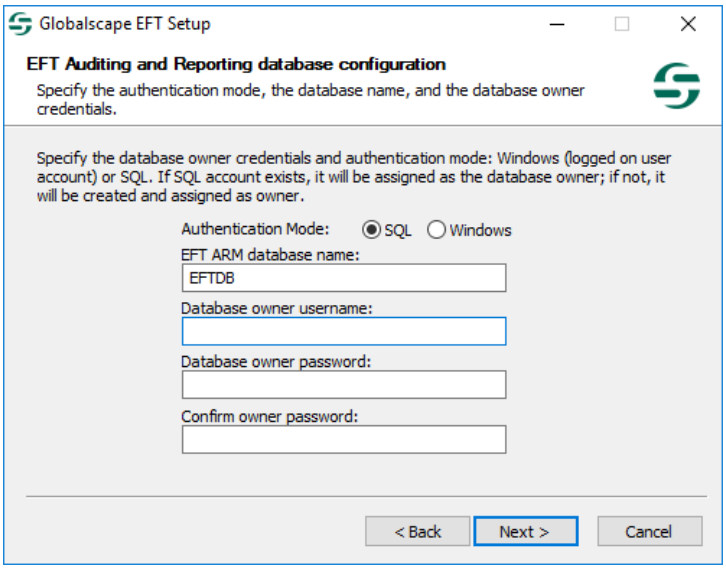
a. Click **Create a new schema**. The configuration page appears.



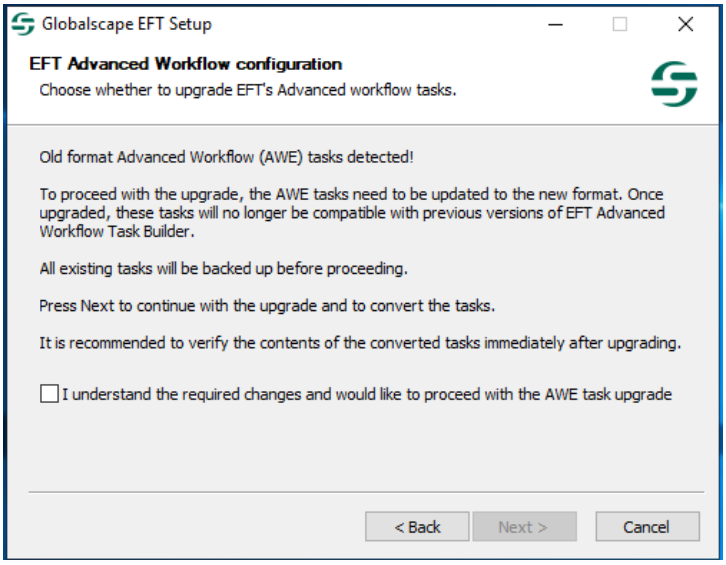
b. Specify the database host address and the EFT-specific schema name and database administrator credentials, and then click **Test**or **Next** to test the connection to the database. (If you have installed Oracle Database Express Edition (XE) for testing/demo purposes, the instance name is XE and the User Name is SYSTEM.)

- If the test fails, click **Back**to verify the configuration or click **Next**and then **Next**again to open the Oracle Technology Network download page and download "Oracle Data Access Components for Windows" driver, if necessary.

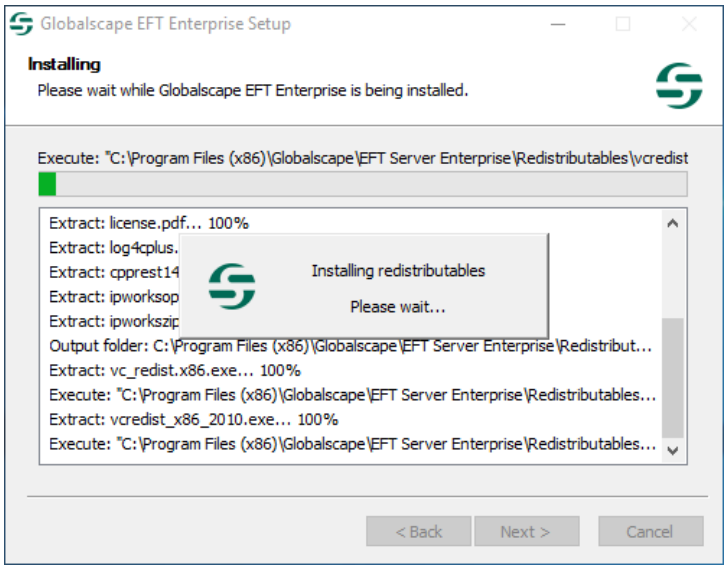
15. After the test is successful, click **Next**. The ARM schema owner credentials page appears.



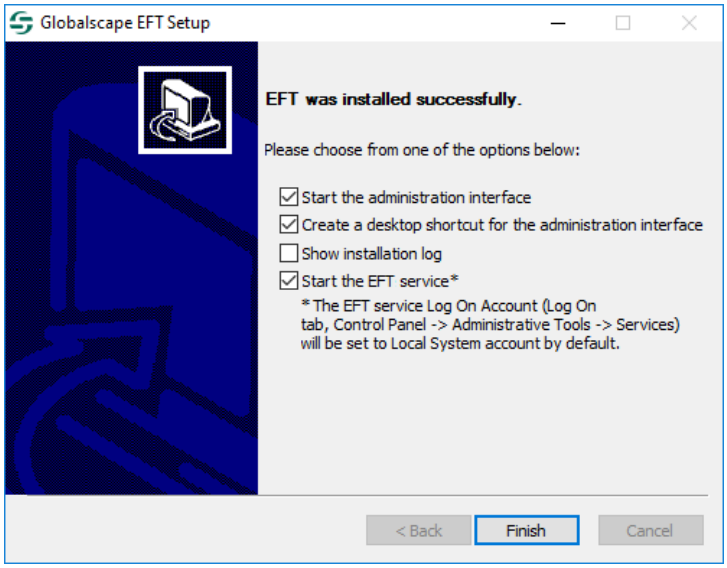
16. Specify or create the ARM schema owner credentials, then click **Next**. The installer creates the tables.
17. If this is not the first installation of EFT, the EFT Advanced Workflow configuration page appears.



The installer installs the options that you've selected, then the **Installation Complete** page appears.



18. Click **Next**. A page appears allowing you to start EFT, create a shortcut to the administration interface on the desktop, open the administration interface, and/or view the EFT version history.

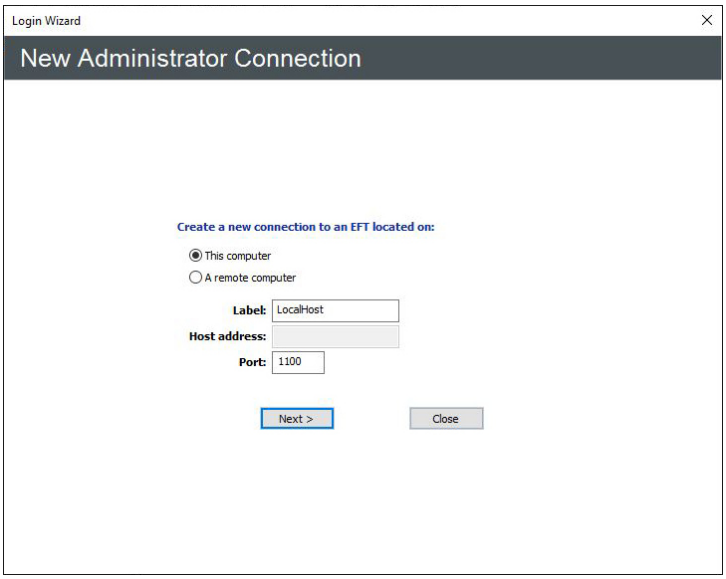


- **Start the administration interface** - If you want to open the administration interface, select the check box. You can also open the interface from the **Start** menu.
- **Create a desktop shortcut** - An administration interface shortcut is created on the desktop by default. If you do not want to create a shortcut, clear the check box.

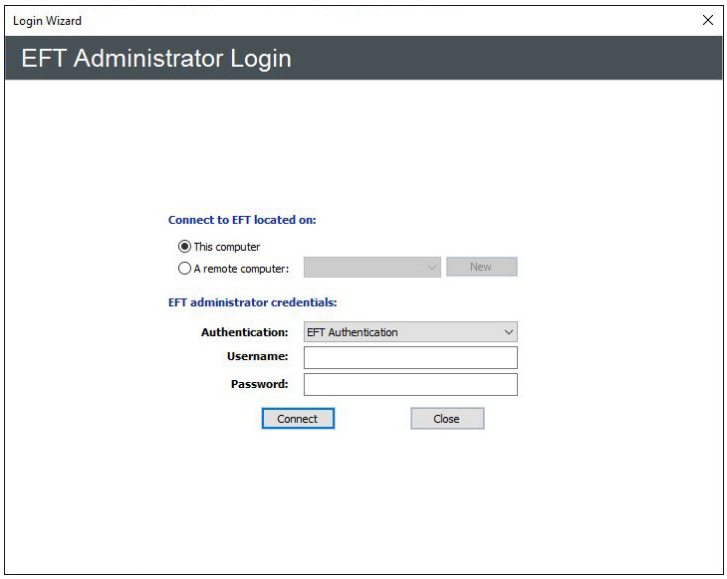
- **Show installation log** - If you want to review the installation log now, select the check box. If you want to review it later, it is stored in a temporary folder, **C:\Program Files\GlobalSCAPE\EFT Server\Installer.log**.
- **Start the EFT Server Service** - Select the check box if you want to start the EFT service when you click **Finish**. The EFT service Log On Account is set to "Local System account."

  IMPORTANT: After it is installed, EFT has access to local folders and files. To run EFT as a service with permissions to the network and mapped drives, you must create an NT account, assign the EFT server service to the account, and log EFT on as a service. Security policies should allow user accounts to log in locally. You can edit the settings for that account as described in Windows Account for the EFT Service.

19. Click **Finish**. If the administration interface check box was selected and the EFT service was started, the **Login Wizard**appears.



20. With **This computer**selected, click **Next**. (You must create a local connection first. Then later you can create remote connections, if you want.) The **EFT Server Administrator Login** page appears.



21. Click in the **Authentication**box and specify the type of authentication to use for this login. Future connections will default to the authentication type that you specify during this initial login, but you can choose a different type. Authentication types include:
    - **EFT Authentication**- Choose this option to log in with an EFT-specified administrator account, such as the one you created during installation.
    - **Integrated Windows Authentication** - Choose this option to log in with an Active Directory or local Windows account.
    - **Windows NET logon**- Choose this option to log in with a local Windows account.
22. In the **Username**and **Password** boxes, provide the login credentials that you created during installation, and then click **Connect**. The **Welcome**page appears. Since you have not yet activated the software, the "Free Trial" reminders appear. After you activate, you will not see the reminder prompt.

Next Steps:

- If you are evaluating the software or just do not want to activate yet, click **Start Trial**, then follow the prompts to Configure EFT.
- If you want to restore EFT configuration from a backup, refer to Backing Up or Restoring Server Configuration.
- If you have purchased a license, click **Activate Now**, then follow the procedures for activating the software.
- Set Windows System Services (You do not have to activate the software before you do this. All features and modules are available during the trial.)

The EFT service runs under a user account, which must have full administrative rights to the folder in which you install EFT. With administrative rights, the EFT service can save all of your settings. **If the service does not have administrative rights, you will lose settings and user accounts whenever you restart the EFT service and you will need to reset permissions on the computer on which the EFT service is running.**

If you are using Microsoft IIS on the same computer as EFT, refer to Running EFT and Microsoft IIS on the Same Computer.

Installing the Advanced Workflow Module

The Advanced Workflow module (AWM) is installed with Fortra's EFT Server and is included in the 15-day trial of EFT, during which you can create, edit, and execute powerful workflows using the EFT Event Rule system. After the trial has expired, you can still create new workflows and edit existing ones; however, after the trial expires, you will no longer be able to execute the workflows with EFT Event Rules. After you purchase and activate a serial numberfor the module, you will once again be able to use the workflows in Event Rules. The workflows are not deleted until you delete them.

EFT subscription licenses have a week-long grace period in which the module will continue to function after being expired. Automate does not have this week-long grace period. When the Advanced Workflow module (AWM) expires from a subscription license and enters its grace period, the Automate side will expire with no grace period; the AWM module will stop functioning in its grace period.

IMPORTANT: If you are upgrading from a version of EFT before v8.2, please read Upgrading the Advanced Workflow Module. There are numerous items that you need to know BEFORE you upgrade, such as the conversion of Advanced Workflow AML files.

Installing the Administration Interface Remotely

When you install EFT, you also install the administration interface. After you have installed EFT and the administration interface on one computer, you can also install the administration interface on remote desktops. You do not need a separate license for each installation of the administration interface.

- The necessary DLL files are also installed and registered when you install the interface remotely, in case you plan to use the COM API remotely.
- For help using the COM API, refer to the online help for the COM API.

This procedure is for installing only the administration interface on a computer that is remote from EFT.

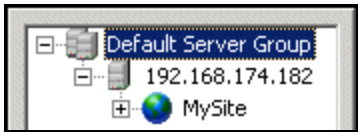
To install EFT and the administration interface on the same computer, refer to Installing the Server, Interface, and Modules.

To install the administration interface remotely

1. Close all unnecessary applications so that the installer can update system files without rebooting the computer.
2. Start the installer, and then click **Next**.
3. After installation components are loaded, the **Welcome** page appears.
4. Read the **Welcome**page, and then click **Next**. The **License Agreement** page appears.
5. Read the license agreement, and then click **I agree** to accept it. (Clicking **Cancel** aborts the installation.) The **Choose Components** page appears.
6. To install **only**the administration Interface, clear the **EFT Server** check box, and then click **Next**. The **Choose Install Location**page appears.
7. The default installation location appears in the **Destination Folder** box. Leave the default or click **Browse** to specify a different folder, and then click **Next**. The **Configuration data path**page appears.
8. Leave the default or click **Browse**to specify a different folder, and then click **Next**. The **Choose Start Menu Folder**page appears.
9. Keep the default shortcuts, specify an existing folder, or type a name for a new folder, and then click **Next**. The administration interface installs.
10. When installation is complete, click **Next**.
    - Leave the **Start the administration interface** check box selected so that you can configure a connection to the remote EFT next.

- If you want to create a desktop shortcut for the administration interface leave the **Create a desktop shortcut** check box selected.
- If you want to review the version history in your default text editor, select the **Show version history** check box.
- If you want to display the installation log, select the **Show installation log** check box.

11. Click **Finish**. The administration interface appears and the **EFT Server administrator Login** wizard appears.
12. Click **A remote computer**, then ensure the remote EFT's IP address appears in the drop-down list. If the remote EFT's IP address does not appear in the list, ensure you can connect to it from this computer and that remote administration is allowed on EFT. Otherwise, click **New**and configure the remote connection.
    - In the **Label**box, provide a name for the EFT to which you want to connect. You can call it anything you want; it has nothing to do with EFT's computer name. This name will appear in logs and reports.
    - In the **Host address**box, type the IP address of EFT computer.
    - In the **Port**box, type the port number used by EFT for remote connections.
13. Click **Next**. The **EFT Administrator Login**page appears.
14. Click the **Authentication**box and specify the type of authentication to use for this login. Future connections will default to the authentication type that you specify during this initial login, but you can choose a different type. Authentication types include:
    - **EFT Authentication**- Choose this option to log in with an EFT-specified administrator account.
    - **Integrated Windows Authentication** - Choose this option to log in with an Active Directory or local Windows account.
    - **Windows NET logon**- Choose this option to log in with a local Windows account.
15. In the **Username**and **Password** boxes, provide the login credentials that you created during installation, and then click **Connect**. The **Welcome**page appears.
    - If connection was not successful, verify the IP address and port on which EFT listens for connections, that remote administration is enabled on the server, and that SSL is properly configured, if used, on EFT.
    - If connection was successful, the remote Server appears in the tree.



Active-Active HA Cluster—Installing or Upgrading the Server

Refer to the Globalscape Knowledgebase article #11271for information about installing or upgrading the server in an active-active, high availability (HA) configuration.

See also Upgrade HA Nodes with Zero Downtime.

Active-Passive Failover Clustering--Installing or Upgrading

Refer to Globalscape Knowledgebase article #11146for details of installing or upgrading the server in an active-passive failover configuration.

Installation Logging

The installation log file is intended for debugging purposes and contains messages that may help resolve issues that arise during installation.

- During installation and maintenance, the installer creates an **Installer.log** file in the **%TEMP%\<Product Name>**directory. For example:
  - **C:\Users\administrator\AppData\Local\Temp\EFT Server\Installer.log**
  - **C:\Users\administrator\AppData\Local\Temp\EFT Server\Installer.log**
- At the completion of the installation, either due to success or failure, the installer copies the final log to the **<InstallDir>\logs** directory, if it exists. If the installer fails during an initial clean installation, the **<InstallDir>\logs**directory may not exist. In this case, the final log file remains in the **%TEMP%\<Product Name>**directory.
- The installer attempts to append to the existing log file on subsequent runs of the installer (for example, if the user performs a Reinstall). It does this by copying any existing **Installer.log**file from the installation directory into the Temp directory, writing to it during installation, and then copying it back to the **<InstallDir>\logs**directory when the installation is finished.
- You can write out the same log messages to another log file of your choosing using the **/logfile=<Log file>** command line switch to the installer.

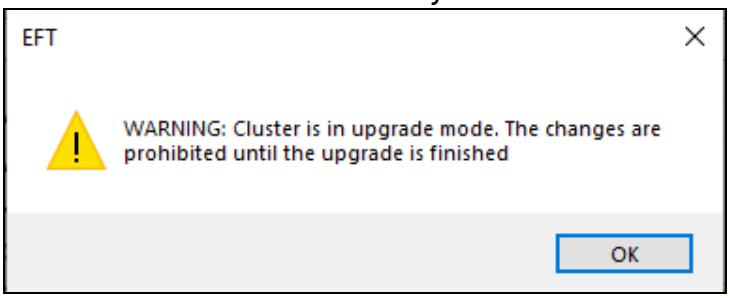
Debug Logging

The installer is capable of writing the same messages that go to the Main Installer Log using the Windows debug logging infrastructure. These messages may be viewed using a utility such as SysInternal's DebugView application. To enable this logging, the installer must be run from the command line with the **/debug** switch.

Upgrade HA Nodes with Zero Downtime

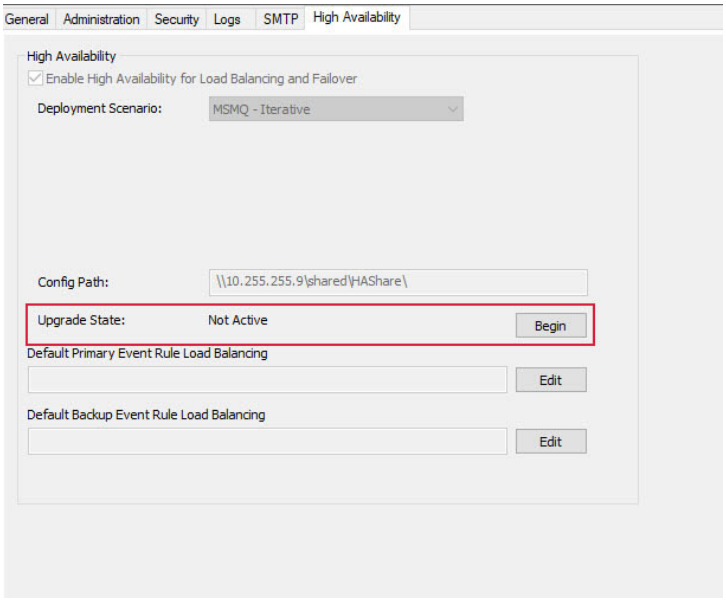
EFT administrators can upgrade their HA nodes with "zero downtime," meaning you can upgrade a cluster without stopping all nodes at the same time.

NOTE: The warning prompt "Cluster is in upgrade mode" is thrown when a user makes a configuration change and then refreshes the EFT administration interface while the server is in "read only" mode.



The Server > HA tab is used to manage the cluster upgrade state

- The button will be displayed as **Begin** when upgrades have not been started.



- The button will be displayed as **End** when upgrades have been completed. Administrators can execute the End state at any point, but nodes that have not been upgraded will fail to start until they are upgraded.
- When enabling the upgrade, EFT administrators will be prompted with a

warning that the transition and change cannot be undone.

- The warning prompt should reference details to review documentation.

To upgrade all of the HA nodes at that same time—without stopping any nodes

In the EFT administration interface, on the **Server > High Availability** tab, you must manually put the cluster into the **Upgrade** state, upgrade each node one by one, then after the upgrade has completed successfully, manually transition the cluster back to **Normal** state.

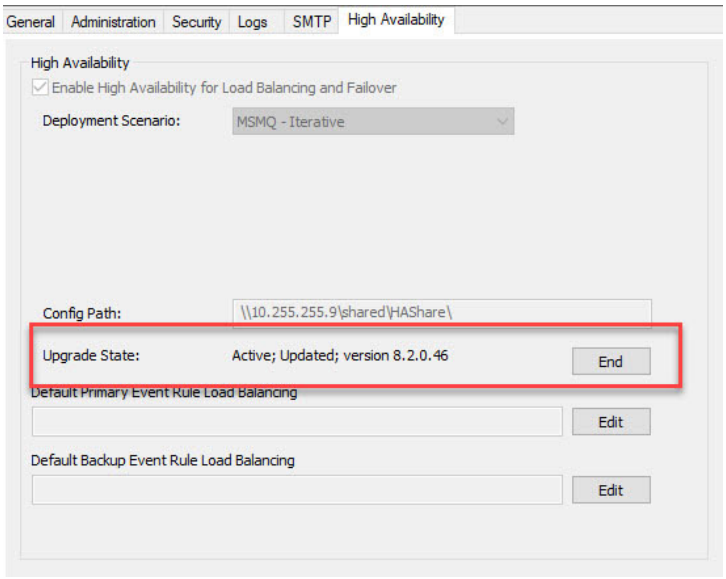
- **Upgrade State**. Allows simultaneous updates to nodes that have an **Outdated** version.

  Upgrade state limitations:

  - Backup/Restore feature is prohibited
  - No configuration changes are allowed during the Upgrade state, except moving the cluster back into the Normal state
- **Normal State**. Requires all nodes have the same version. Upon transition to Normal, the Upgrade State will display “Not Active”

  Normal state limitations:

  - Loading old nodes is prohibited. EFT will not start when the nodes are not upgraded.
  - You will be unable to transition from Upgrade to Normal when an upgrade has not been completed. This only affects nodes that have not been upgraded.
  - EFT will prevent COM API from transitioning from Upgrade to Normal state. A proper response code/error will be presented
  - EFT will prevent REST API from transitioning EFT from Upgrade to Normal state. A proper response code/error will be presented.
  - When upgrade has ended (at the global level or a node that was upgraded), for any nodes that were not upgraded, the EFT Server Service will stop and fail to start until they are upgraded.
  - Transition state from Upgrade to Normal are global, which affects all nodes within the cluster, so administrators should only end upgrades after all nodes have been upgraded.



Upon successful HA upgrade to a new version, the **High Availability** tab's **Upgrade State** will display “Active; Updated; x.x.x.x”, where x.x.x.x is the newer version of EFT (the version to which EFT was upgraded).

Normal state to Upgrade state

- All nodes are Outdated. Admin logins to any of the nodes and enter the cluster into the "Upgrade" state (with GUI/COM/REST).
    - EFT admins shall be able to transition from Normal to the Upgrade state via our EFT administrator interface High Availability tab.
    - EFT admins shall be able to transition from Normal to the Upgrade state via COM. Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade.
    - EFT admins shall be able to transition from Normal to the Upgrade state via REST API. Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade.
    - The ability to start the Upgrade state is a global setting; once set at any node, all nodes will report the same state.
    - Upgrade state should be used ONLY when upgrading to a new version of EFT and not when an EFT administrator forgets to upgrade a node in the cluster from a previous upgrade.
- Once configured for Upgrade, the cluster is in Upgrade state, and you can upgrade each node one by one.

- Outdated nodes write audit data to local *.sql files only; Each node will have their own local *.sql file.
- Updated nodes write into ARM database; If no SQL schema changes exist, there is a post process in the Normal state that will migrate the data from the *.sql file into the ARM database.
- Uses Web folder appropriate to node's version.
    - The nodes' version should match the same version.
    - Shadowfax folder will be copied from \\<HASharedPath>\Web to \\<HASharedPath>\UpgradeFromx.x.xx (where x.x.x.x is the older EFT version); This …\UpgradeFromx.x.x.x will be used for Outdated nodes.
    - Shadowfax folder \\<HASharedPath>\Web will be used for Updated nodes and will be updated with the first upgraded node.
- Outdated nodes allow admins to login in read-only mode. EFT administrators will not be able to make any configuration changes to EFT.
- Updated nodes allow admins to login in read-only mode AND move the cluster to Normal state.
- Configuration changes write in deltas only (there could be only internode mx messages).
    - Changes are not saved into the configuration files, ServerConfig.db and SiteConfigXX.db files. (Part of the advanced property HAFullConfigDumpIntervalMins.)
    - Internode mx messages are communications between EFT nodes (no QA validation).
- Unknown internode messages are ignored; These are internal nodes for Outdated nodes that may not know about freshly added internode messages in Updated nodes.
- Cluster Management subsystem doesn't send any messages and ignores all received messages.
- ERLB subsystem doesn't delegate to run any event rules - all rules are processed with Master node only. Client connections to the server will be processed without any restrictions during the Upgrade state.

Upgrade state to Normal state

- All nodes are Updated. Admin will need to log into any node and end the upgrade which will switch it back to Normal state (with GUI/COM/REST)

    - EFT admins shall be able to transition from Upgrade to Normal state via our EFT Admin UI
    - EFT admins shall be able to transition from Upgrade to Normal state via COM; Appropriate error message(s) will be provided if enabling Normal state on any node when the cluster is already configured for Normal
    - EFT admins shall be able to transition from Upgrade to Normal state via REST API; Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade
    - The ability to end the upgrade state is a global setting; once set at any node, all nodes will report the same state. Nodes that were not upgraded and the upgrade state has ended, will fail to start.
    - Nodes that were not upgraded after the Upgrade state ends, now Normal, can be upgraded later and will be visible and continue to work in the cluster
- Normal state limitations: Loading old nodes is prohibited. EFT will not start when the nodes are not upgraded

COM has several methods to manage cluster upgrade state

- Enum: HAUpgradeNodeState
    - NotInUpgrade = 0,
    - OldNode,
    - NewNode
- Method: ICIServer::GetHAUpgradeNodeState; Retrieves node upgrade state
- REST has two endpoints to manage cluster upgrade state:
    - Get HA node upgrade state; GET /server/ha/upgrade
    - Changes entire HA cluster state to the upgrade or normal state: POST /server/ha/upgrade

Related Topics

- Active-Active HA Cluster Installing or Upgrading the Server
- HA FAQ
- High Availability Tab of a Server

Upgrading EFT and Modules

For a successful upgrade, it is important to understand the changes between your current version and the version you are upgrading to. In some cases, you will need to do a "stepped" upgrade, as you can't upgrade directly from some older versions to the current version.

EFT v8.1 and later support upgrades only from v8.0.5, v8.0.6, and v8.0.7. The EFT installer will prevent you from upgrading if it detects an installed version that is not supported in the v8.1 upgrade path

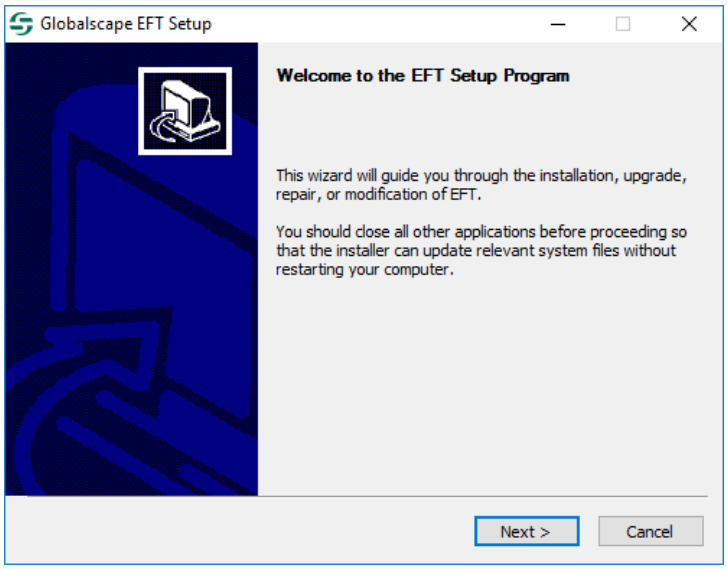
IMPORTANT: The Advanced Workflow Engine (AWE), based on Automate Desktop v10, is now the Advanced Workflows Module, based on Automate 2024. ***BEFORE*** upgrading EFT and its modules, refer to Upgrading the Advanced Workflow Module for details of issues to be aware of, such as converting AML files.

- If you are upgrading a cluster node, refer to Active-Passive Failover Clustering--Installing or Upgrading or Active-Active HA Cluster - Installing or Upgrading the Server .
- Upgrade an HA Cluster with Zero Downtime

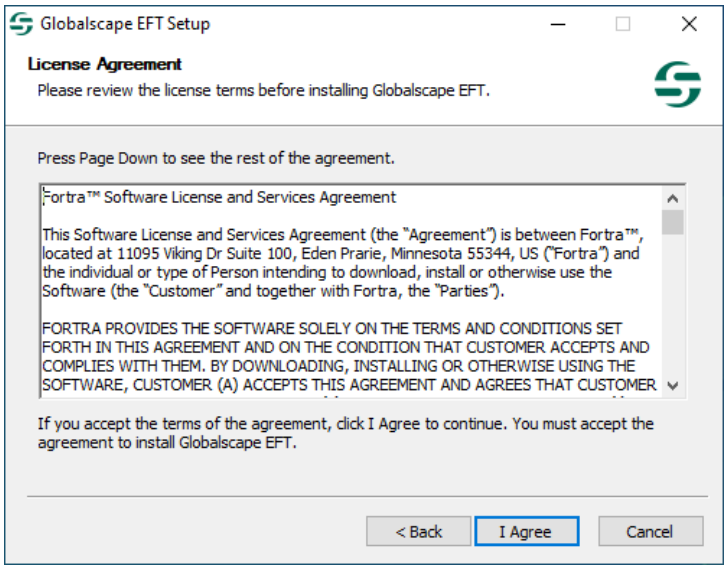
IMPORTANT: Customers using the Remote Agent module must install a patched version of 8.2.0 before upgrading to v8.2.1. Failure to do so will cause Remote Agent upgrades to fail and will require manual intervention to upgrade. Contact Support for details before upgrading.

To upgrade EFT and its modules

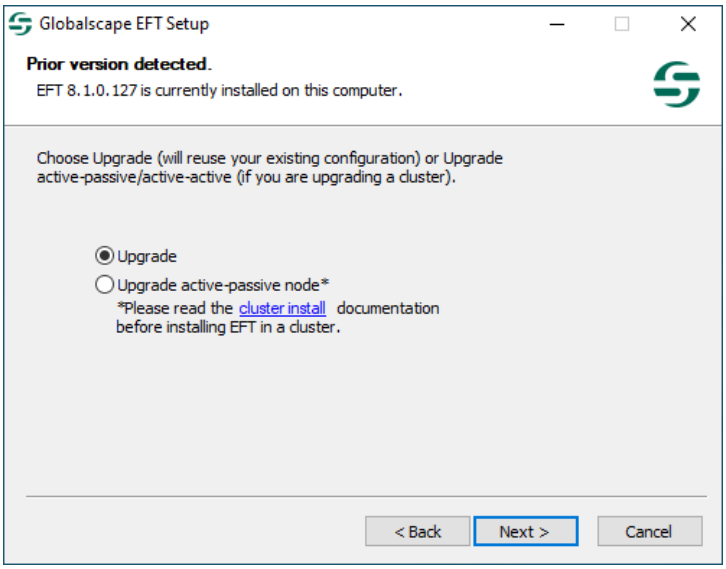
1. Close all unnecessary applications so that the installer can update system files without rebooting the computer.
2. Start the installer. The **Welcome** page appears.



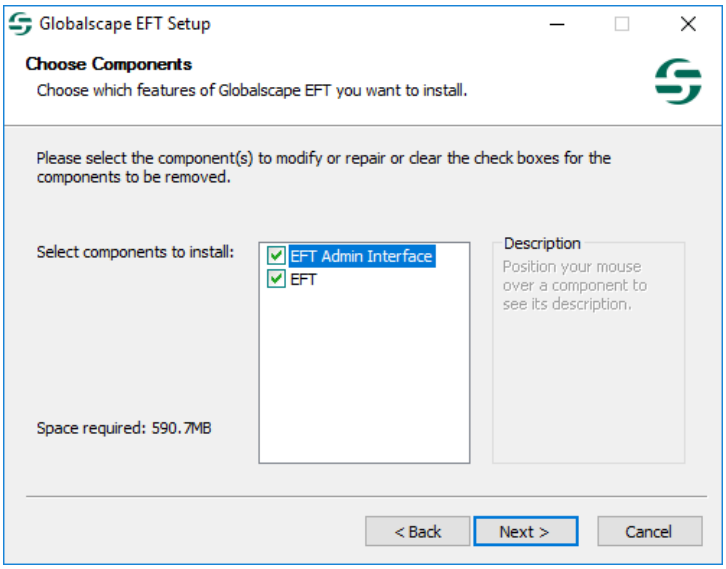
3. Read the **Welcome**page, and then click **Next**. The **License Agreement** page appears.



4. Read the license agreement, and then click **I agree** to accept it. Clicking **Cancel** aborts the installation.
    - If you are upgrading or reinstalling, the version detected page appears.

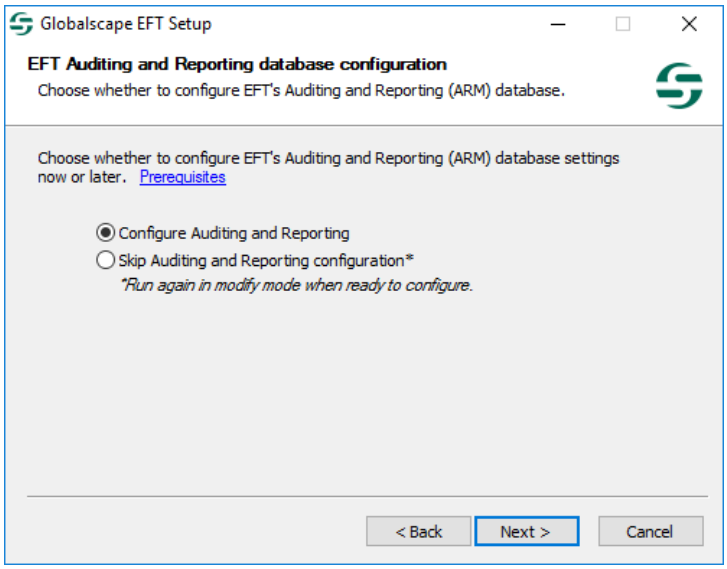


5. Click **Upgrade** then click **Next**. The **Choose Components** page appears.



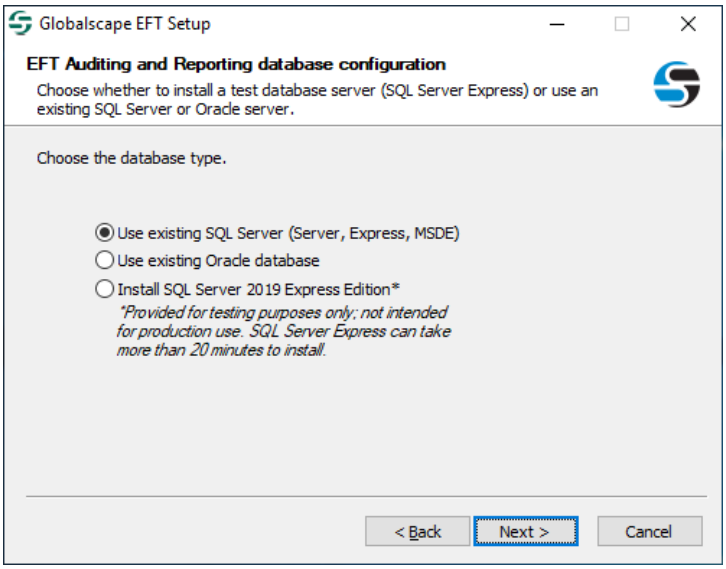
When you install EFT, the **EFT administrator Interface** check box must also be selected. After you have installed EFT and the administration interface on one computer, you can install the administration interface on other computers for remote administration. (To install the administration interface on a remote computer, refer to Installing the administration Interface Remotely.)

6. Click **Next**. The ARM selection page appears.

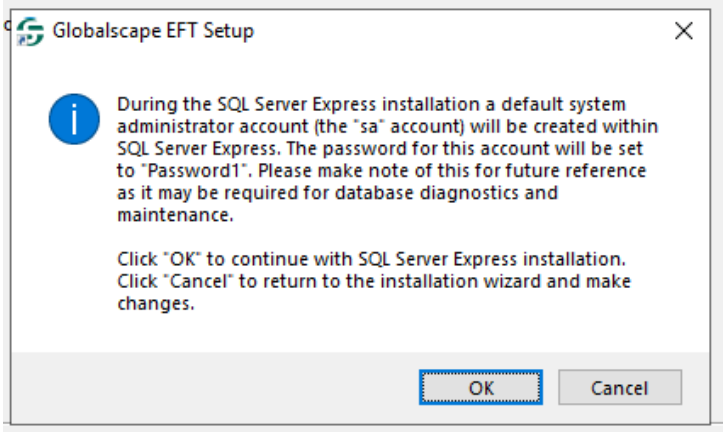


- If you want to configure auditing and reporting, click **Next**.
- If you do not want to configure auditing and reporting, click **Skip auditing and reporting configuration**, and then click **Next** to skip the database configuration pages. You can still configure the database later, if you want.
- If you want to manually create the database later, click **Skip auditing and reporting configuration**, and then refer to Manually Creating the ARM Database in SQL Server or Manually Creating the ARM Database in Oracle when you're ready to create the database.

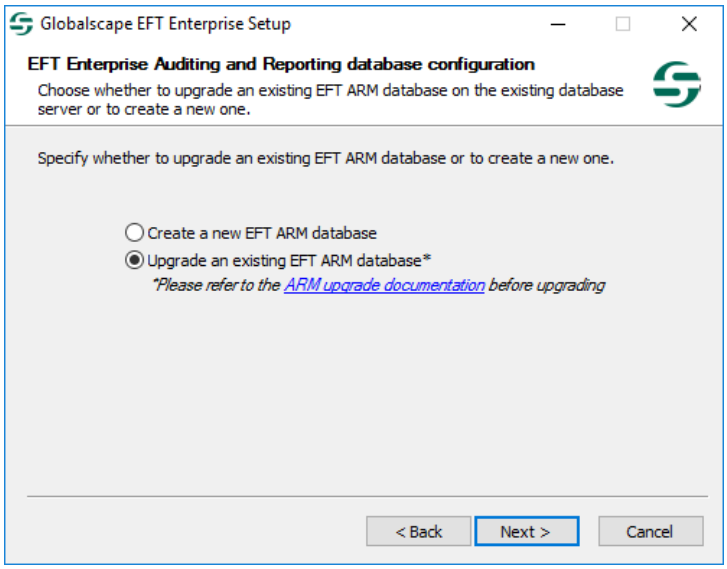
7. Specify the type of database, SQL Server or Oracle, that EFT is to use. You will need the connection information available to point EFT to the database. If you already have a database to use, then you do not need to install SQL Server Express. (If you are using the "no db" installer, you will not see the "Install SQL Server" option.)



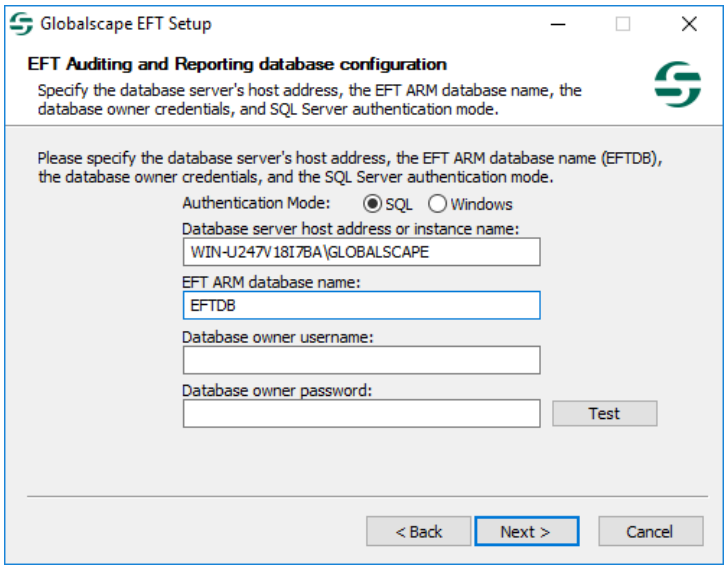
- **Install SQL Server Express**
  - SQL Server Express is provided for use in a trial. It is not intended for production use. During installation, a default system administrator account (the "sa" account) will be created within SQL Server Express. The password is set to Password1.



  - Click **OK**to continue SQL Server Express installation and follow prompts to complete SQL Server Express installation.
  - Once the SQL Server Express installation begins, you can't cancel it. The only way to stop it is to reboot the computer.
- **Use existing SQL Server**:



a. Click **Use an existing EFT ARM database**. The configuration page appears.

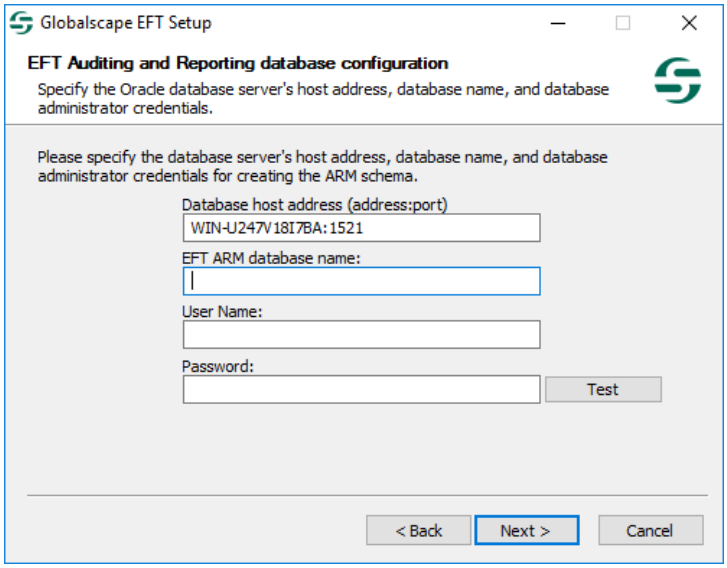


b. Specify **Windows**or **SQL** Authentication. (**Windows** mode allows you to connect through a Microsoft Windows user account. **SQL**allows you to connect using either Windows Authentication or SQL Server Authentication.)
c. Specify the host address or instance name.
d. Specify the database server SA or privileged user account name (for example, sa).
e. Specify the database server SA or privileged user account password.

f. (Optional) Click **Next**or **Test** to test the connection to the database. If the test fails, click **Yes** to verify database connection details or **No** to continue without configuring the database.

- **Use existing Oracle database:**

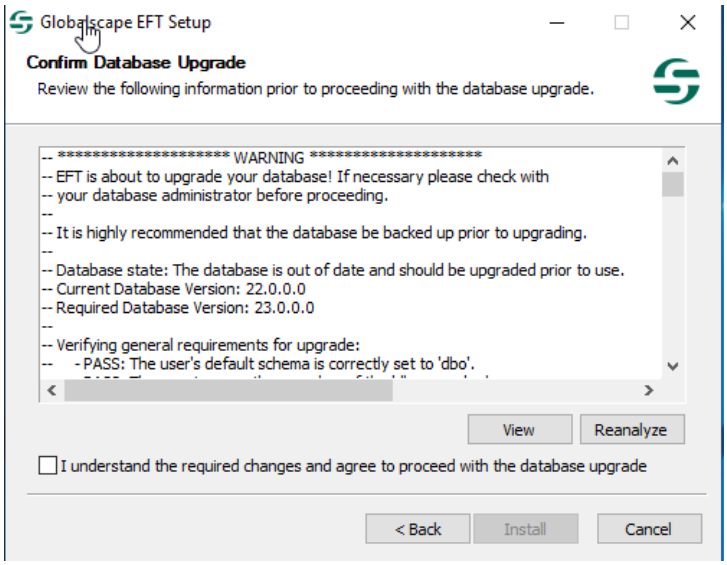
a. Click **Create a new schema**. The configuration page appears.



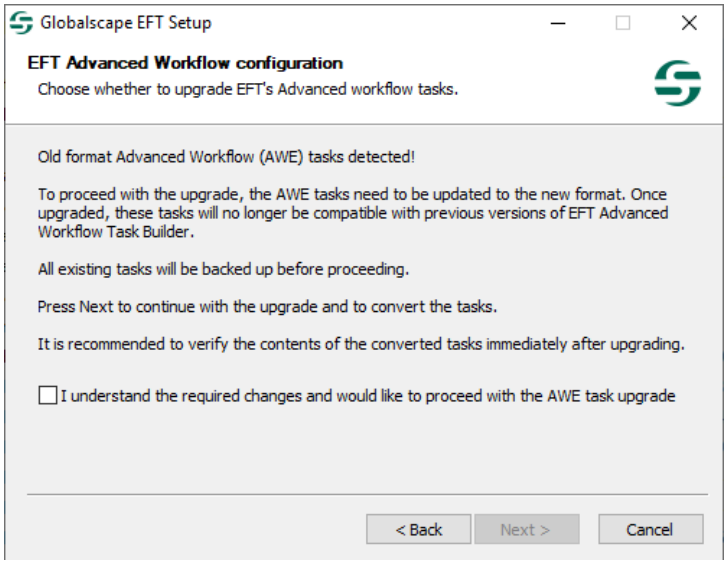
b. Specify the database host address and the EFT-specific schema name and database administrator credentials, and then click **Test**or **Next** to test the connection to the database. (If you have installed Oracle Database Express Edition (XE) for testing/demo purposes, the instance name is XE and the User Name is SYSTEM.)

- If the test fails, click **Back**to verify the configuration or click **Next**and then **Next**again to open the Oracle Technology Network download page and download "Oracle Data Access Components for Windows" driver, if necessary.

8. After the test is successful, click **Next**. The **Confirm Database Upgrade** page appears.

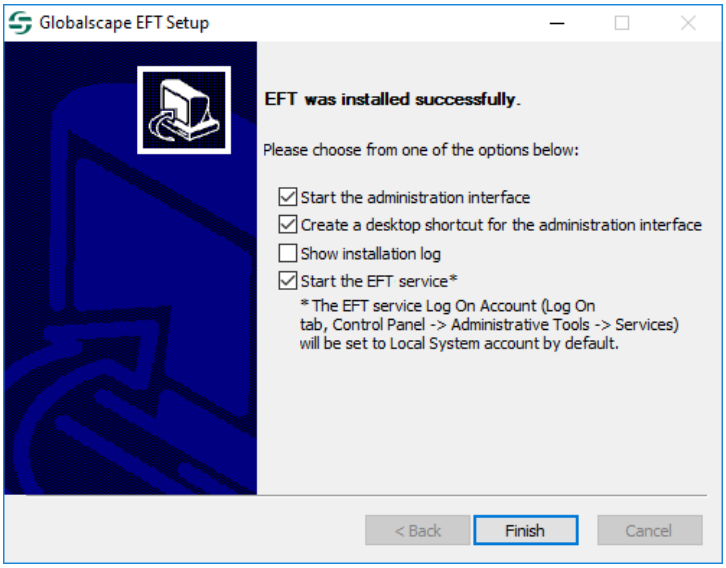


9. The database version information is displayed.
    - Click **View** to open a TXT file of the database upgrade details and save the file for later, if needed.
    - **Reanalyze** compares the new database information to the old and displays it on the page.
    - Select the **I understand...** check box to continue, then click **Install**.
    - After the database has been upgraded, the **Old format Advanced Workflow task detected** page appears.



    - Select the **I understand the required changes...** check box, then click **Next** to proceed with the upgrade.
    - Click **Install**. When installation is complete, a **Completed** page appears.

10. Click **Next**. On the final page, select or clear check box to start the administration interface, create a shortcut to the administration interface on the desktop, show the installation log, and/or start the EFT server service.



11. Click **Finish**.

Uninstalling the Software

Uninstalling EFT removes everything installed in the **Program Files\Globalscape** folder. It does not uninstall configuration files, Oracle or SQL Server tables, Reports, or Backup files in **\ProgramData\Globalscape\EFT Server**. (To see \ProgramData\, open Windows File Explorer, click **View**, then select the **Hidden Items** check box.)

To remove EFT

1. Click **Start > Programs (Apps) > Globalscape > EFT > Uninstall EFT**. The **Uninstall** wizard appears.
2. Click **Uninstall**. The uninstalling progress page appears.
3. After the program files are removed, the **Uninstallation Complete** page appears. Your license information remains in the Windows Registry, in case you decide to reinstall. Click **Close**.

For a "Clean" Uninstall

After uninstalling above is complete, you can clean up any leftover files manually. Some files are left behind in case you want to reinstall EFT. The table below lists the various folders, files, and registry settings that can be removed if you don't plan to reinstall EFT.

- The EFT uninstall wizard does not affect the database. If you want to purge the database, do that **before deleting\ProgramData\Globalscape\EFT Server** because that is where the purge scripts are stored.
- Uninstalling EFT removes everything installed in the **\Program Files\Globalscape\EFT Server** folder. It does not uninstall configuration files, Oracle or SQL Server tables, Reports, or Backup files.
- Your license information remains in the Windows Registry, in case you decide to reinstall.
- For HA installations, there will be configuration and EFT user files in the shared location.

Artifact Type	Artifact Default Location	Description
Database tables	ARM database; ODBC Authentication (SQL Server or Oracle)	Database-specific purge scripts are installed with EFT. The scripts are installed under the "SQL Server" and "Oracle" sub-directories of the **\ProgramData\Globalscape\EFT Server\ directory.**
Folder\Files	\Program Files\Common Files\Globalscape	Directory where application is installed
Folder\Files	\ProgramData\AutoMate	Directory where Advanced Workflow Engine files are installed
Folder\Files	\ProgramData\Globalscape	Directory where application configuration and site information is stored
Folder\Files	\Users\<usernames>\AppData\Local\GlobalSCAPE\	administrator user files; delete if no longer needed
Folder\Files	\Users\<usernames>\AppData\Roaming\GlobalSCAPE\	administrator user files; delete if no longer needed
Folder\Files	\inetpub\EFTRoot	EFT user files; delete if no longer needed
Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Globalscape	You can delete the entire **Globalscape** folder (if you have no other Globalscape products)
Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GlobalSCAPE Inc	You can delete the entire **Globalscape Inc** folder (if you have no other Globalscape products)
Registry	HKEY_CURRENT_USER\Software\Globalscape	You can delete the entire **Globalscape** folder (if you have no other Globalscape products)
Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Computer\HKEY_LOCAL_MACHINE\SOFTWARE\AutoMate	Automate files; You can delete the entire **Automate** folder
TEMP folders	Temp location of account used for EFT service and Temp location of user running EFT installer	temporary files

Related Topics

- Upgrading the Software
- Modifying or Repairing the Installation

Silent Command-Line Installation

Let's suppose you have several computers around the world on which you want to install EFT. You can provide to each of the remote sites an installation file with a batch file, then ask a local administrator to execute the batch file, which will install EFT. The script silently installs or upgrades EFT without any interaction on the part of the administrator. The installer logging functionality can be used to verify the outcome and diagnose potential issues. You can also upgrade silently from the command line and install the administration interface from a command line.

> **NOTE:** If you install EFT HA via the silent installer, then, once configured, if you upgrade EFT via the install wizard, EFT fails to start the server service. The install wizard is setting the EFT server configuration details to the default paths. This issue only occurs when you use the silent installer for the initial deployment, then follow with an upgrade using the wizard. If you use the wizard for both installing and upgrading, or the silent installer for both installing and upgrading, this issue does not occur. Refer to the Upgrading EFT topic for more information.

> **NOTE:** At this time, the silent install parameters do no apply to subscription installations and upgrades.

Command line usage

```
installer.exe /S /USERNAME= /PASSWORD= [/APPDATA=] [/D=]
```

where /S = silent installation and /USERNAME = administrator user name

Optional parameters examples:

```
/APPDATA = appdata path
(default = "C:\ProgramData\Globalscape\EFT Server")

/INSTALL_SQLEXPR =(y/n, Y/N)
/NOAUTOSTART = If present, service will not automatically start
when installation is complete
```

Batch File Examples

- If you are installing EFT without a database at the default path:

```
eft-nodb.exe /S /USERNAME=test /PASSWORD=test
```

- If you are installing EFT at the default path with SQL Express:

```
eft.exe /S /USERNAME=admin /PASSWORD=alaska /INSTALL_SQLEXPR=y
```

- Skip launching of the EFT Windows service that typically occurs at the end of installation, reinstallation, upgrade, or database settings modification:

```
/NOAUTOSTART
```

- Do not install the full server. Install only the files needed for the administration interface:

```
eft.exe /S /USERNAME=admin /PASSWORD=africa /aionly /debug
```

- Use an alternate location for EFT application data:

```
eft.exe /S /USERNAME=admin /PASSWORD=africa /APPDATA=c:\eft data
dir
```

- Set installation directory:

```
/D=D:\Program Files\GlobalSCAPE\EFT Server
```

- Instruct the installer to install only the stand-alone server; do not install the trial database that is included in the installer
- /D=<path> -- If used, this must be the last parameter used in the command line and must not contain any quotes, even if the path contains spaces. Only absolute paths are supported.

```
/S
/USERNAME=<username>
/PASSWORD=<password>
```

Optional Parameters

```
/D=<path>
/debug
/aionly
/CLUSTERNODE=<option>
/APPDATA="<DATA_PATH>"
/NOAUTOSTART
```

HA Cluster Example

- /NOAUTOSTART should be configured after /S and before any other commands
- Licenses should be added before passing any HA configuration parameters
- Any folder paths for AppData or SharedConfigPath should be encapsulated in quotes when spaces exist

```
eft-8.1.0.16_nodb.exe /S /NOAUTOSTART /USERNAME=EFTAdmin
/PASSWORD=!D5f5ns51 /EFTUSER="1234567"
EFTLICENSE="A12345678" /PGPLICENSE="AQERQERQR"
/WSLICENSE="ASFJOAJROWFOQ" /HACLUSTERNODE=1
/MULTICASTPORT="8001" /APPDATA="D:\Program
Files\GlobalSCAPE\EFT Server\Config"
/SHAREDCONFIGPATH=\\njfile01\Shared\EFTSharedConfig
/D=C:\Program Files\GlobalSCAPE\EFT Server\
```

Parameters must be in the following order:

Command/Switch	Example
Silent Command	/S
Login	/USERNAME=test /PASSWORD=!x12345abcdef
Which node this is	/HACLUSTERNODE=1
Which PORT to use for this EFT HA cluster	/MULTICASTPORT="8052"
Where your default data will be stored	/APPDATA="C:\Program Files\GlobalSCAPE\EFT Server\Config"
The location from which both nodes will pull the mutual configuration	/SHAREDCONFIGPATH=\\vmware-host\Shared Folders\EFTSharedHAConfig\Config
Where the binaries go	/D=D:\Program Files\GlobalSCAPE\EFT Server\

Administration Interface-Only Installation

This path will instruct the installer to install the administration interface without installing EFT. This is useful if you want to do remote administration of EFT. (This path is only applicable when the Server is not installed on the same computer.)

Required Parameters

```
/S
/aionly
```

Optional Parameters:

/D=<path> -- If used, this must be the last parameter used in the command line and must not contain any quotes, even if the path contains spaces. Only absolute paths are supported.

Silent Upgrade

The installer can also be run in silent mode for upgrades. The Silent upgrader only works if EFT was installed using silent installation.

To do a silent upgrade of EFT

1. Close all instances of EFT administration interface, both local and remote connections.
2. At the command prompt enter the following command:

```
eft-nodb.exe /S
```

The executable exits silently (without notification) and the upgrade continues in the background.

After several minutes, the silent upgrade process will complete and the EFT server service will be automatically restarted.

A record of the upgrade can be found in the EFT installation directory file **Installer.log**.

> **NOTE:** ARM must be upgraded separately, because the silent installer will not upgrade ARM. The “/INSTALL_SQLEXPR” flag does not work with doing a silent install upgrade.

Command-Line Parameters

The installer supports specification of the following command line parameters. When running the installer in silent mode, using the /S switch, these parameters are used to specify both the required and optional values as detailed in Parameter Definitions.

Parameter Definitions

- /S
  - Applicable installation types: active-active, active-passive, standalone
  - Description: Initiates a silent installation.
  - Default: The installer defaults to graphical user interface mode.
  - Example: /S
- /D=<path>
  - Applicable installation types: active-active, active-passive, standalone
  - Description: The installation directory.
  - Default: C:\Program Files\Globalscape\EFT
  - Example: /D=C:\Program Files\GlobalSCAPE\EFT Server
- /debug
  - Applicable installation types: active-active, active-passive, standalone
  - Description: Enables logging to the Windows system debug log. This log may be viewed in real time using tools such as DebugView that is part of the SysInternals Suite from Microsoft.
  - Default: Disabled by default
  - Example: /debug
- /aionly
  - Description: Do not install the full server. Install only the files needed for the administration interface.
  - Default: The installer deploys both the administration interface and EFT by default
  - Example: /aionly
- /APPDATA="<DATA_PATH>"
  - Applicable installation types: active-active, active-passive, standalone
  - Description: Use an alternate location for EFT application data

    - Default: EFT usually writes application data to the OS standard location C:\ProgramData\Globalscape\EFT Server Example: /APPDATA=C:\EFTData
- /CLUSTERNODE=<option>
    - Applicable installation types: active-passive
    - Description: This install will be part of an active-passive cluster.
    - Options:

      /CLUSTERNODE=1 - This is the primary

      /CLUSTERNODE=2 - This is not the primary
    - Description: This install will be part of an active-passive cluster.
    - Example: /CLUSTERNODE=1
- /HACLUSTERNODE=<option>
    - Applicable installation types: active-active
    - Description: This install will be part of an active-active cluster.
    - Options:
        - /HACLUSTERNODE=1 - This is the first node in the cluster.
        - /HACLUSTERNODE=2 - This is not the first node in the cluster.
    - Default: Default installations are non-clustered
    - Example: /HACLUSTERNODE=1
- /PASSWORD=<password>
    - Applicable installation types: active-active, active-passive, standalone
    - Requirements: Must be used in conjunction with the /USERNAME switch
    - Description: The password to use for the initial administration account.
    - Default: None
    - Example: /PASSWORD=wkBG2YxgzBpR
- /DMZGW="<EFT site>/<DMZ host>/<DMZ port>|…"
    - Applicable installation types: active-active, active-passive, standalone
    - Description: Specify the gateway(s) for given EFT site(s) on the current node.
    - Example: /DMZGW="MySite/192.168.10.210/44500|Site2/192.168.10.210/44500"
- /NOAUTOSTART

    - Applicable installation types: active-active, active-passive, standalone
    - Description: Skips launching of the EFT Windows service that typically occurs at the end of installation, reinstallation, upgrade, or database settings modification.
    - Default: Service automatically starts on new installs
    - Example: /NOAUTOSTART
- /INSTALL_SQLEXPR=<option>
    - Description: Whether to install the bundled MSSQL Express Installer
    - Options: Y - Install the bundled MSSQL Express; N - Do not install the bundled MSSQL Express
    - Prerequisites: Can only be used with EFT installs that contain a bundled SQL Express installer.
    - Example: /INSTALL_SQLEXPR=Y
- /NOREQS
    - Applicable installation types: active-active, active-passive, standalone
    - Description: If specified, the installer will skip checking of the common prerequisites that occurs during initial installer launch. This setting is mainly used for debugging purposes, or when the checks have errors that are preventing a valid install in the field.
    - Check #1 - Check for Minimum OS
    - Check #2 - Check if user currently has administrator privileges
    - Check #3 - Check if DMZ is installed
    - Check #4 - As of EFT 6.5 Unicode DotNet 4.0 FULL is a requirement
    - Check #5 - EFT is of two prior versions
    - Default: The common prerequisites will be checked by default
    - Example: /NOREQS
- /logfile=<file>
    - Applicable installation types: active-active, active-passive, standalone
    - Description: Log installation messages to the specified file (this is in addition to theinternal log that is always created by the installer).
    - Default: None
    - Example: /logfile=C:\Temp\EFTInstall.log
- /SkipValidateSQLServerPassword
    - Description: By default, the installer will validate the EFT Server administrator password against the SQL Server Express password requirements (e.g., the Windows account password policy plus some

additional illegal keywords). This option provides a way to instruct the installer to skip this validation check.
    - Default: Disabled by default
    - Example: /SkipValidateSQLServerPassword
- COHERENCEQUEUE="<name>"
    - Applicable installation types: active-active
    - Description: Use an alternate name for EFT's coherence queue.
    - Default: EFTCoherenceQueue
    - Example: /COHERENCEQUEUE=NewCoherenceQueueName
- /EVENTQUEUE="<name>"
    - Applicable installation types: active-active
    - Description: Use an alternate name for EFT's event queue.
    - Default: EFTEventQueue
    - Example: /EVENTQUEUE=NewEventQueueName
- /MULTICASTADDRESS="<ip>"
    - Applicable installation types: active-active
    - Description: Use an alternate multicast address for MSMQ.
    - Default: 234.1.1.1
    - Example: /MULTICASTADDRESS="234.9.9.9"
- /MULTICASTPORT="<port>"
    - Applicable installation types: active-active
    - Description: Use an alternate multicast port for MSMQ.
    - Default: 8001
    - Example: /MULTICASTPORT="9999"
- /MSMQMulticast
    - Set to 0 indicates the HA installation uses unicast, otherwise multicast is used. Default is 1. (In EFT v7.4.2 and later)
    - Product and module registration parameters
    - Applicable installation types: active-active, active-passive, standalone
    - Example (registering EFT Enterprise): /EFTLICENSE="A92463BH4RY7"
- /REGISTRATIONPROXY="<ip>:<port>"
    - Description: If registering during installation, specify the ip and port of the proxy to send registration traffic through.
    - Default: not used
    - Example: /REGISTRATIONPROXY="192.168.100.248:3128"

- /EFTUSER=”<name>”
  - If product registration is performed during installation, this name will be used to register all modules for which serials are provided.
  - Example: /EFTUSER=“John Doe”
- /HACLUSTERNODE=<option>
  - Applicable installation types: active-active
  - Description: This install will be part of an active-active cluster.
  - Options:1.This is the first node in the cluster; 2.This is NOT the first node in the cluster
  - Default: Default installations are non-clustered
  - Example: /HACLUSTERNODE=1
- /SHAREDCONFIGPATH=“<SHARED_PATH>”
  - Applicable installation types: active-active nodes
  - Description: Specify the location of an active-active cluster’s shared configuration data.
  - Default: none
  - Example: /SHAREDCONFIGPATH=\\host\sharedfolder
- /USERNAME=<username>
  - Applicable installation types: active-active, active-passive, standalone
  - Description: The username to use for the initial administration account.
  - Default: None
  - Example: /USERNAME=EFTAdmin

Registration Parameters

Register EFT Server first before you register any module licenses.

> **NOTE:** The Advanced Authentication Modes module doesn't register in the Silent Installer. You can register it in the EFT administration interface after installation.

- /EFTLICENSE=“<serial>”
  - Registers EFT server during installation.
- /ACCLICENSE=“<serial>”
  - Registers Acceleration module during installation. (Only in EFT v7.2.3 - 7.4.7.13)
- /ADVAUTHLICENSE=“<serial>”

    - Registers the Advanced Authentication Modes module (AAMM).
- /ARMLICENSE=”<serial>”
    - Registers ARM during installation.
- /AS2LICENSE=”<serial>”
    - Registers AS2 during installation.
- /AWELICENSE=”<serial>”
    - Registers AWM during installation.
- /CICLICENSE=“<serial>”
    - Registers the Content Integrity Control features
- /CCMLICENSE=“<serial>”
    - Registers Cloud Connector Module (CCM). (EFT v7.4.4 and later)
- /DMZSINGLELICENSE=“<serial>”
    - Registers single-site DMZ during installation.
- /DMZMULTILICENSE=“<serial>”
    - Registers multisite DMZ during installation.
- /EALICENSE="<serial>"
    - Registers the Enterprise Actions module (EAM).
- /FMELICENSE="<serial>"
    - Registers the Folder Monitor event
- /FORMSLICENSE
    - Registers the Secure Forms module.
- /FTCLicense=“<serial>”
    - Registers the File Transfer Client.
- /FTPSLICENSE=“<serial>”
    - Registers the FTPS module license
- /HALICENSE=“<serial>”
    - Registers the HA license
- /HTTPSLICENSE
    - Registers the HTTPS module. (EFT v8.1 and later)
- /MTCLICENSE=”<serial>”
    - Registers the MTC during installation.
- /PGPLICENSE=”<serial>”
    - Registers the OpenPGP module during installation.
- /RAMLICENSE =“<serial>”

    - Registers the Remote Agent Module (RAM). (EFT v7.4.4 and later)
- /RCLICENSE =“<serial>”
    - Registers the Regulatory Compliance module (EFT v8.1 and later)
- /SFTPLICENSE
    - Registers the SFTP module. (EFT v8.1 and later)
- /TELICENSE =“<serial>”
    - Reisters the Timer event. (EFT v8.1 and later)
- /WSLICENSE=”<serial>”
    - Registers the Workspaces module. (EFT v8.0.7 and later)

Debug Logging

The installer is capable of writing the same messages that go to the Main Installer Log using the Windows debug logging infrastructure. These messages may be viewed using a utility such as SysInternal’s DebugView application. To enable this logging, the installer must be run from the command line with the **/debug** switch.

After You Are Done

Congratulations! EFT is now installed.

Next steps:

- Review Configuration and Security Best Practice for helpful configuration tips and recommended settings.
- Read the following topics for additional information about your next steps.
  - Creating and Configuring an EFT Server
  - Configure the First EFT Connection
  - Activate the Software (EFT and Modules) (You will need your license keys.)
  - Create a Windows Account for the EFT Server Service
  - Backing Up or Restoring Server Configuration
  - Modifying or Repairing the Installation
  - Promoting EFT Stand-Alone to Cluster Node
  - Upgrading the Software
  - Upgrade an HA Cluster with Zero Downtime
  - Uninstalling the Software
  - HA Nodes Configuration File

Configuration and Security Best Practices

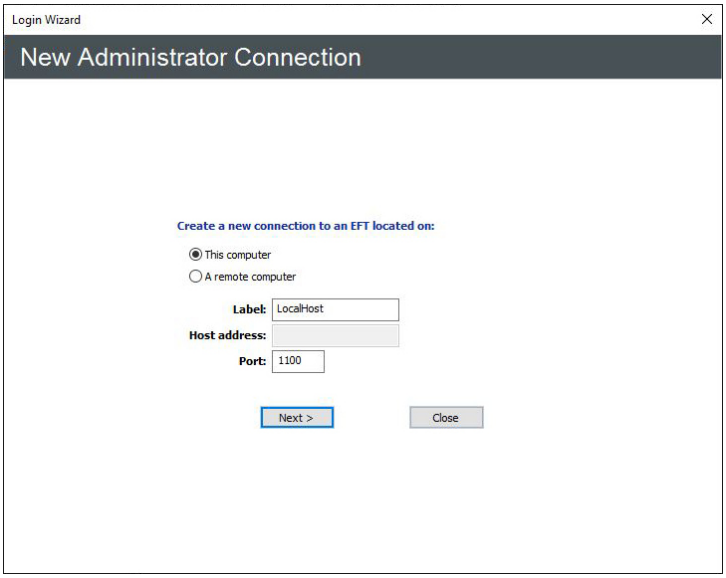
Refer to Globalscape Knowledgebase article #11312for details about configuration and security best practices.

Configure the First EFT Connection

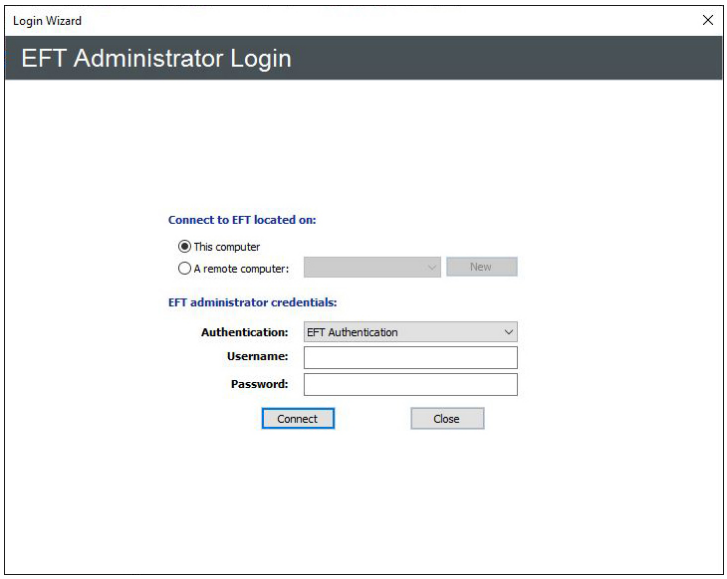
You must first configure the local connection before you can configure a remote location.

To configure EFT on the local computer

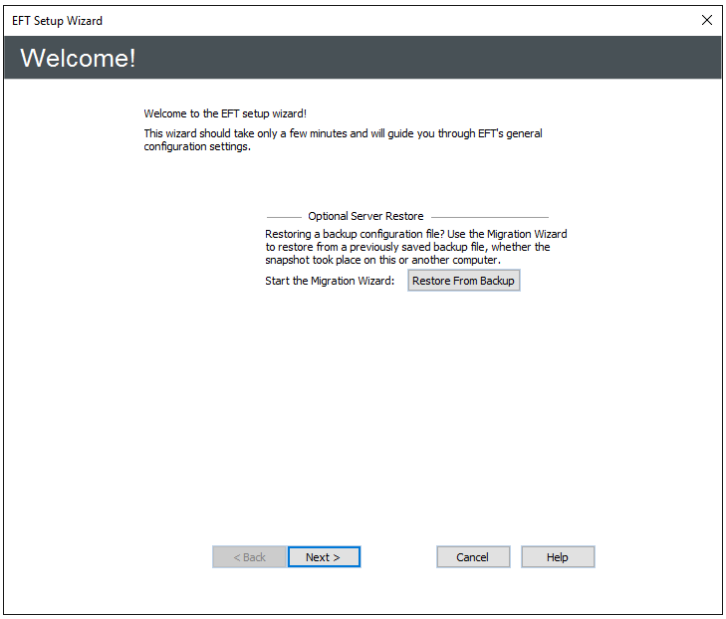
1. After installationis complete, the **New Administrator Connection** wizard appears. (If you have already defined a connection and want to create another one, refer to **Creating a Remote Connection**.)



2. Leave **This computer**selected, then specify the **Label**for the local connection. By default, the label is `LocalHost`. Because LocalHost is a very common label, it is a good idea to change the label to something that is easily identifiable in error logs, reports, and remote connections. For example, `GS_EFTS`. You can label EFT anything you want; the EFT name is ***not*** dependent upon the computer name. The **EFT Administrator Login**page appears.

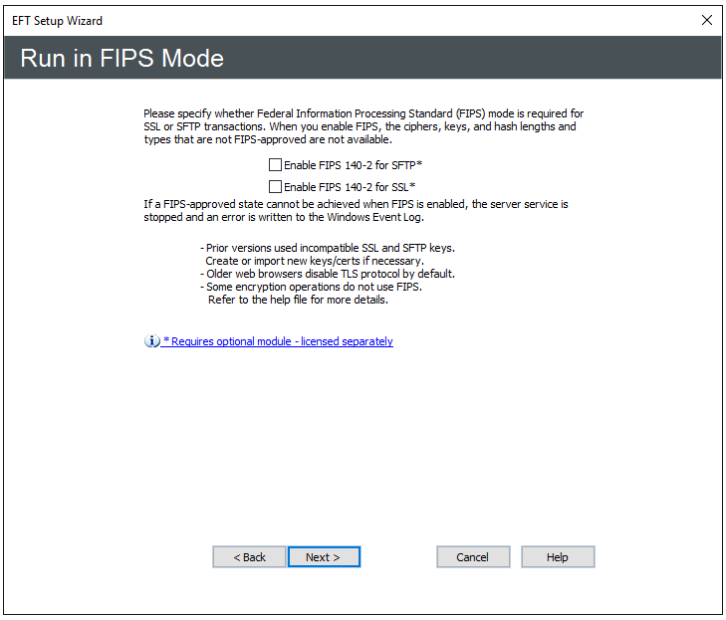


3. Click the **Authentication**box and specify the type of authentication to use for this login. Future connections will default to the authentication type that you specify during this initial login, but you can choose a different type. Authentication types include:
    - **EFT Authentication**- Choose this option to log in with an EFT-specified administrator account, such as the one you created during installation.
    - **Integrated Windows Authentication** - Choose this option to log in as the currently logged on user (Integrated Windows Authentication).
    - **Windows Authentication**- Choose this option to log in using a specific Windows account.
4. If you specified **EFT Server Authentication** or **Windows Authentication**, in the **Username**and **Password** boxes, provide the login credentials that you created during installation. The **Welcome** page appears. Because you have not yet activated the software, the "Free Trial" reminders appear. After you activate, you will not see this prompt.
5. Do one of the following:
    - If you are evaluating the software or just do not want to activate yet, click **Start Trial**, then follow the procedures in Creating and Configuring an EFT Server.
    - If you have purchased a license, click **Activate Now**, then follow the procedures for activating the software.
6. Click **Next**. The **Server Setup** wizard **Welcome** page appears.



- If you are not restoring from a backup, click **Next**.
- If you are restoring from a backup, click **Restore from Backup**, then refer to Backing Up or Restoring Server Configuration for the procedure.

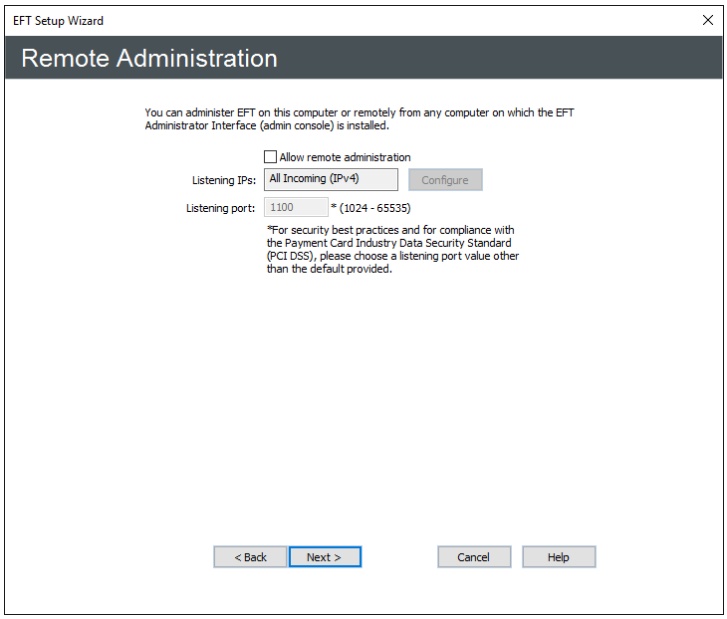
7. Click **Next**. The **FIPS Options** page appears.



When you enable FIPS mode, the ciphers, keys, and hash lengths and types that are not FIPS approved are not available. If a FIPS-approved state cannot be achieved when FIPS is enabled, the EFT service is stopped and an error is written to the Windows Event Log.

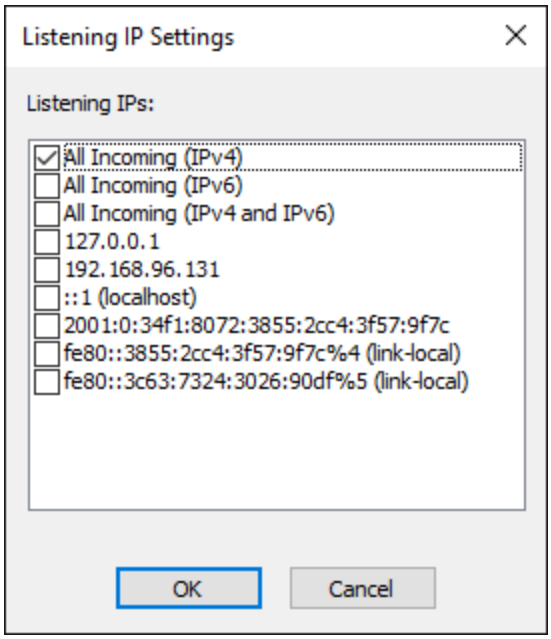
- To use FIPS for SFTP (SSH2), select the **Enable FIPS for SFTP** check box. To use FIPS for SSL, select the **Enable FIPS for SSL** check box.
- A confirmation prompt appears when you select either check box. When you enable FIPS, the EFT service must be restarted. Click **OK** to continue with FIPS enabled or click **Cancel**if you do not want to use FIPS and restart the EFT service.

8. Click **Next**. The **Remote Administration**page appears.



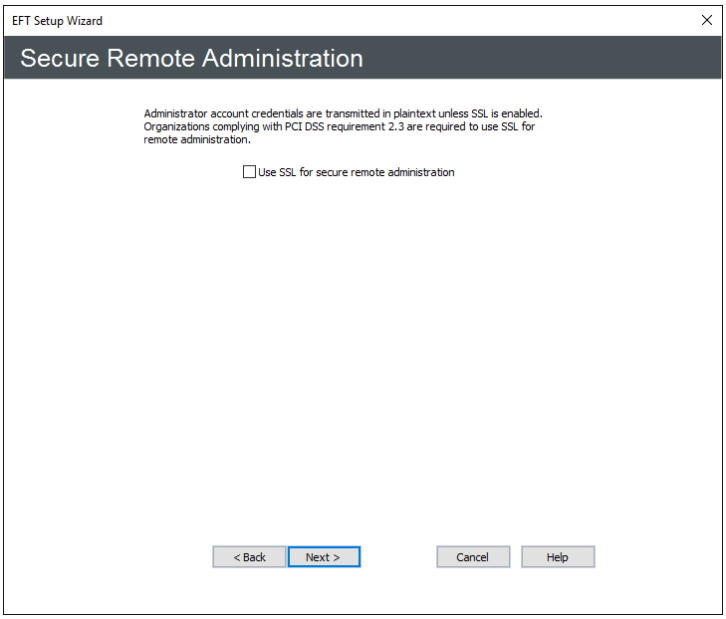
- If you do not want to allow remote administration, clear the **Allow remote administration** check box.
- If you want to allow remote administration:
  a. Select the **Allow remote administration** check box and specify the **Listening IPs**.
  b. Click **Configure**to specify one or more IP addresses. The **Listening**

IP Settings dialog box appears.

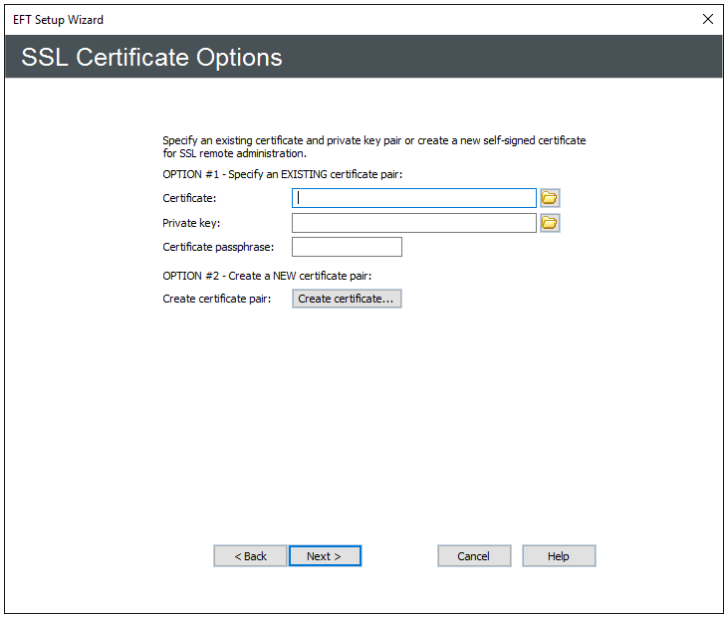


- **All Incoming (IPv4)** is selected by default. Select the check boxes for addresses that you want to allow; clear the check boxes for the addresses that you do not want to allow, then click **OK**.

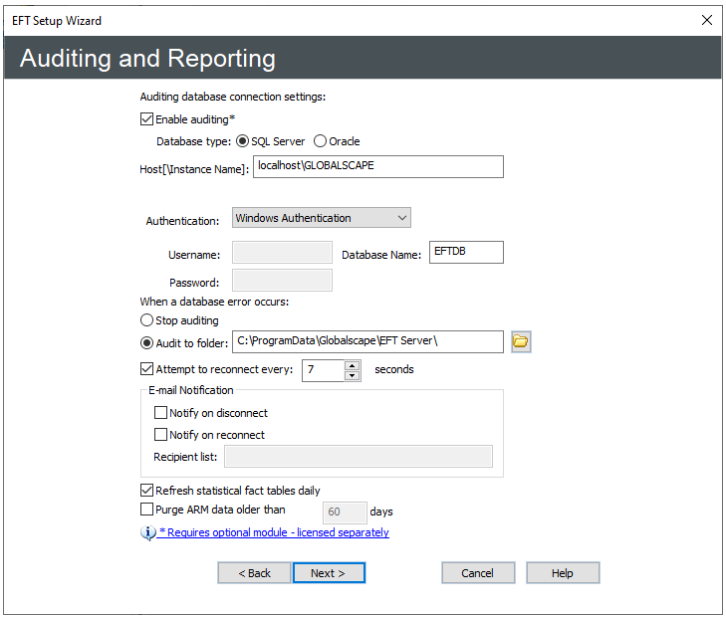
9. Specify the **Listening port**. (For security best practices and compliance with the PCI DSS, specify a port other than the default of 1100.)
10. Click **Next**. If you chose remote administration, the **Secure Remote administration** page appears.



11. Administrator account credentials are transmitted in plaintext unless SSL is enabled. Organizations complying with the PCI DSS are required to use SSL for remote administration. To enable secure remote administration, select the **Use SSL for secure remote administration** check box, and then click **Next**. The **SSL Certificate Options** page appears.



12. Do one of the following:
    - In the **Certificate**and **Private Key** boxes, click the folder icon to browse for the private key pair files.
    - Click **Create certificate** to create one. Refer to SSL Certificate-Based Login, Creating Certificates and Importing a Certificate into the Trusted Certificate Database for information regarding certificates.
13. Click **Next**. The **Auditing and Reporting**page appears.



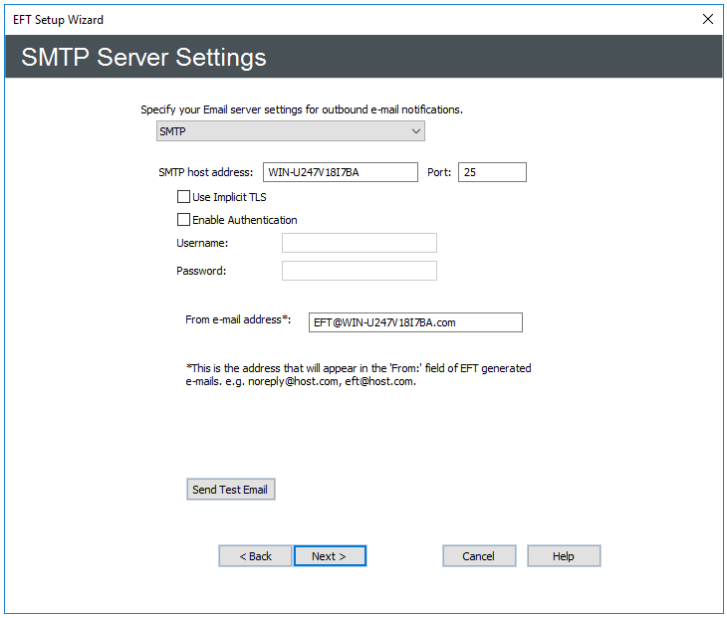
14. If you are using Auditing and Reporting, select the **Enable auditing** check box, then provide the information required to connect to the ARM database as described below. If you are not using Auditing and Reporting, skip to the next step. (Auditing and reporting is a requirement of the PCI DSS.)
    a. In the **Database type** area, specify whether you are using **SQL Server** or **Oracle**for the auditing database.
    b. In the **Host[\Instance Name]** box, type EFT name or IP address.

       If you are using SQL Server as the Auditing Database, **\InstanceName** corresponds to SQL Server's notion of named instances, a feature that allows a given computer to run multiple instances of the SQL Server Database Service. For more information, refer to http://msdn2.microsoft.com/en-us/library/ms165614.aspx

    c. In the **Authentication**box, specify the type of authentication used by the database, either **Windows Authentication**or **SQL Server Authentication**.
       - If you choose **SQL Server Authentication**, you must also specify the "sa" username and password. In the **Username**and **Password** boxes, type the username and password used to connect to the database (***not***the EFT credentials).
    d. In the **Database Name** box, type the name of the database.
    e. In the **In case of audit database error** area, specify an Action for EFT to take if there is an error with the database. To stop recording data, select **Stop auditing**. To continue recording data to a file, select **Audit to folder**, and specify the location for the log file.

UNC paths are supported. The Globalscape Server service must run on a computer that has access to the network share, and the full UNC path must be used, that is: \\xcvd.forest.intranet.xc\Common_Files, **not** G:\Common. IPv6 literals must use the Microsoft-specific IPv6 address form that uses "ipv6-literal.net" for use in a UNC path. (Refer to the Wiki article about IPv6 for more information about IPv6 literals in UNC paths.)

15. To try to recover from a database error automatically, select the **Attempt to reconnect every**check box and specify the frequency in seconds.
16. In the **email notification**area, select the **Notify on disconnect**check box and/or the **Notify on reconnect**check box, and then specify the email address(es) to which EFT is to send database connection error notifications. You can add as many email addresses as needed; separate the addresses with a comma or semicolon. EFT uses its global SMTP email settings from the SMTP Configuration to send the emails. You will configure those settings on the next page.
17. The **Refresh statistical fact tables daily**check box is selected by default. If you do not want the database fact tables to be refreshed as part of EFT's hard-coded nightly cleanup routine (at midnight), then clear the check box.
18. Click **Next**. The specify **SMTP Server Settings**page appears.



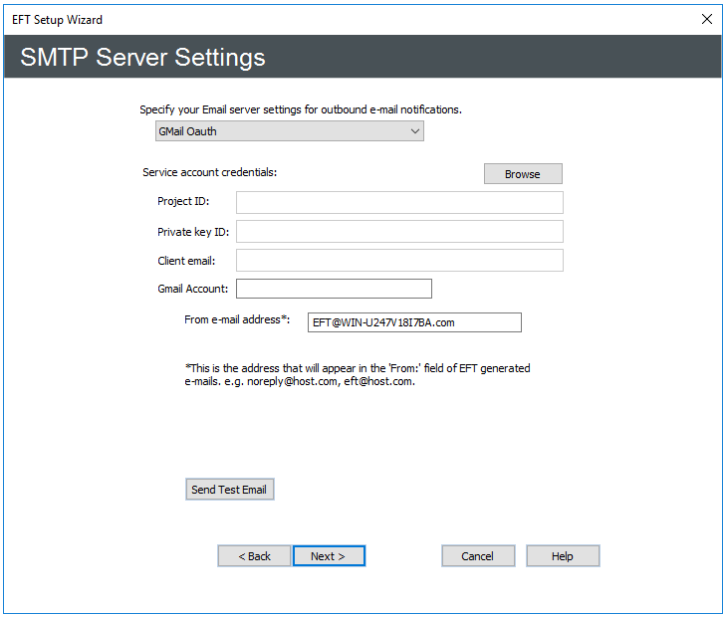
19. To specify your email server settings for outbound email notifications, click the drop-down box and select **SMTP** (default), **GMail Oauth**, or **Office 365 Oauth**. The options on this page of the wizard change based on your selection.

For SMTP

- In the **SMTP host address** boxes, specify the SMTP server host address and port.
- Select the **Use Implicit TLS** check box, if needed.
- If using the SMTP server, select the **Enable authentication** check box and provide the **Username** and **Password**.

> **NOTE:** If you're not sure what to use for credentials, skip this step by selecting **Next** to continue with the server, site, and user setup. Later you can configure SMTP in the administration interface.

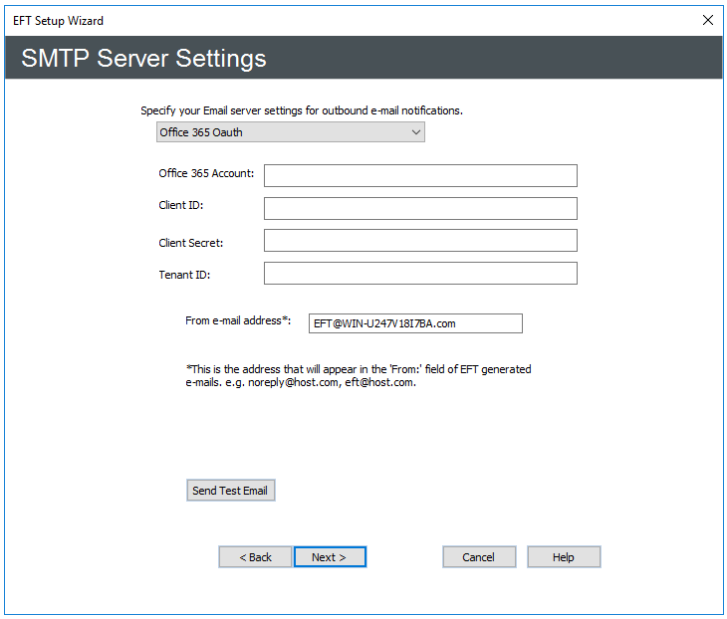
For Gmail Oauth



- In **Service account credentials**, click **Browse** and select the file that contains the **Service account key json path** file. The fields will be completed with the information from the JSON file.

> **NOTE:** For details of using Gmail Oauth service accounts, refer to https://developers.google.com/identity/protocols/oauth2/service-account.

For Office 365 Oauth



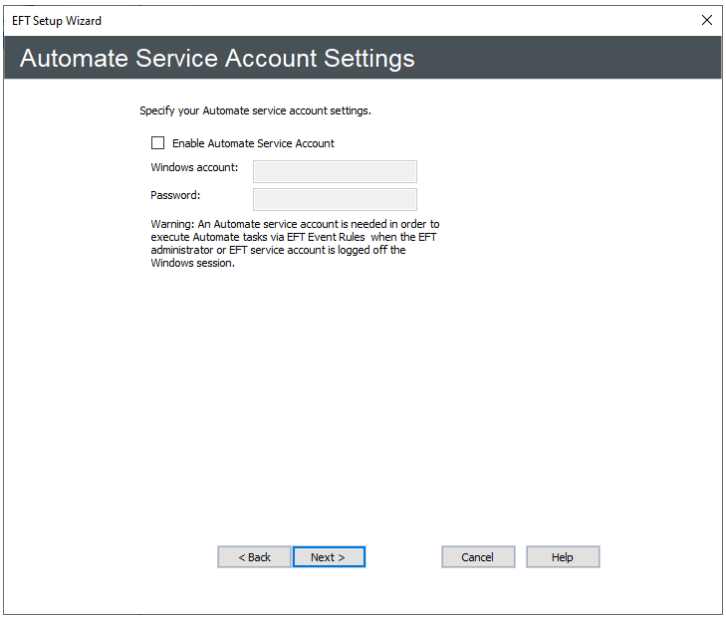
- Complete the fields to connect to the Office 365 mail server:
  - Office 365 Account -
  - Client ID -
  - Client Secret -
  - Tenent ID -

> **NOTE:** Microsoft recommends that you disable SMTP AUTH organization-wide or per mailbox (hosted in Office 365 or Microsoft 365). For more details, refer to the Microsoft topic at https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission.)

20. In the **From email address** box, specify the email address for email notifications (such as those triggered by Event Rules). This is the address that appears in the **From** box of emails sent by EFT. For example, type `noreply@serverhost.com`.

> **NOTE:** The email address syntax is validated when you click **Send Test Email** or **Next.**. If the email address contains invalid characters or does not contain @, an error message appears. Click **OK**to dismiss the error message, then correct the address.

21. Click **Send Test Email** to ensure the credentials are correct.
22. Click **Next**. The **Automate Service Account Settings** page appears.



The Automate Service Account must be enabled and provided Windows account credentials so that the Automated Workflows can continue to run in event rules when the Windows session is logged out or locked or EFT server service account is logged out. Select the **Enable Automatic Service Account** check box and provide the Windows credentials.

23. Click **Next**. Server Setup is complete.

    You are offered the option of continuing to the Site Setup wizard, or quitting the wizard, saving EFT settings, and configuring the Site(s) later. You must configure at least one Site (a virtual host) to service inbound connections to EFT.

24. Click an option, then click **Finish**. If you chose FIPS mode for SSL and/or SSH, prompts appear explaining that EFT has entered FIPS mode. Click **OK**to dismiss the prompts.
25. If you chose **Run the Site Setup wizard now**, the Site Setup wizard **Welcome** page appears.
26. Next, refer to Creating a Site for the procedure for configuring the first Site.

Creating and Configuring an EFT Server

After you follow the procedures Installing the Server, Interface, and Modules, the next step is to log in to EFT via the Server interface, called the *administration interface*or AI, and configure the client connections to EFT. The instructions below describe how to configure the first EFT connection.

***You must configure EFT for the first time on the computer on which the EFT service is installed*.**After you have created the local connection and enabled remote connections, you can connect to and administer EFT remotely.

Even if you plan to restore the Server from a backup, you must still create the initial Server object in the administration interface.

Anytime you connect to the EFT Server service, if no Servers have been defined, the **Server Setup** wizard **Welcome** page appears. The **Server Setup** wizard guides you through EFT configuration or allows you to restore from backup. The wizard helps you configure Server-specific options such as allowing remote administration. After the brief **Server Setup** wizard is completed, you have the option to run the **Site Setup** wizard to configure a Site, and then the **User Setup** wizard to provision a user. (You have to create at least one site for users to be able to connect to EFT.)

You may cancel out of the **Server Setup**wizard anytime by clicking **Cancel**or the **X** in the upper right corner. However, any settings made through the wizard are discarded, except for keys/certificates added to the key manager (by creating or importing).

You will need the following information to create and configure EFT:

- If you are allowing remote administration of EFT and you are using SSL, you need to know the SSL settings and have access to the SSL keys and certificates.
- If you are restricting remote administration to specific IP addresses, you need to know the IP addresses and ports.
- If you are using DMZ Gateway, install and configure DMZ Gateway (on a different computer). The installation and configuration of DMZ Gateway is not *required*before creating Servers and Sites, but the Site setup wizard asks for the DMZ Gateway information. Alternatively, you can configure DMZ Gateway after Site setup is complete, and then provide the DMZ Gateway connection information in EFT's administration interface.

If you are configuring your first EFT Server connection, refer to **Configure the First EFT Connection**. If you are configuring a new, remote EFT connection, refer to **Creating a Remote Connection**.

Activating the Software (Licensing EFT and Modules)

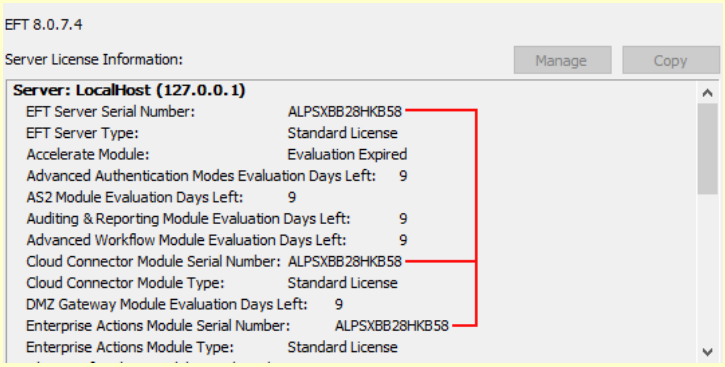
The EFT server with FTP is free, but you should still register your EFT serial number in case you need support. EFT on-premises licenses are available as a perpetual license (register once and never have to register again, except in some upgrade instances), or as a monthly or yearly subscription.

When the trial period ends for modules for which you did not purchase a license, an information error appears in the Windows Event Log to indicate the module has expired.

After you register the EFT license, the **About EFT** dialog box shows that EFT is licensed.

IMPORTANT: When upgrading from v8.0.5 or 8.0.6 to 8.0.7 (in preparation for upgrading to 8.0.7, and then 8.1 or 8.2), it is important to register EFT Server *first* before you register any module licenses.

- When registering a new installation after v8.0.5, it has been found that if you register a module before you register the EFT license, the server will act as though EFT has already been registered. That is, in **Help > About** it will show the module registered, but it will reference the same key as the module that was registered before EFT.



- If you run into an issue where your EFT Server license will not work, please contact support. Do not enter any other serial numbers until EFT has been registered.
- If you register a module without first registering EFT, then our registration process will not work properly and you might have troubles should you need support.
- Registration of EFT with older EFT Server Enterprise or Express serial numbers are supported; this will unlock certain features similar to an upgrade scenario.
- Manual registration of EFT with older EFT Server Enterprise or Express serial numbers is supported, however, we recommend you work with our support team.
- EFT 8.0.7 and later do not support DMZ Gateway single site registration via manual registration.
- Do not use your Automate license key with EFT, as this is managed by EFT's licensing. Having an Automate license does not automatically grant a license in EFT to unlock the Advanced Workflow Module (AWM) in EFT.

Registering EFT and the Modules

You must activate the software with a serial number. Each module is available during the EFT trial and must be activated separately.

- If you are moving an EFT from one computer to another, contact the Globalscape customer service team or your account manager so that we can adjust your account on our activation server. Activation on the new computer will not be possible until the adjustment is made.
- If you are upgrading EFT residing in a clustered environment, refer to Installing EFT in a Cluster and contact Globalscape technical support for assistance, if necessary.
- If you have troubles with activation, refer to manual registration below.

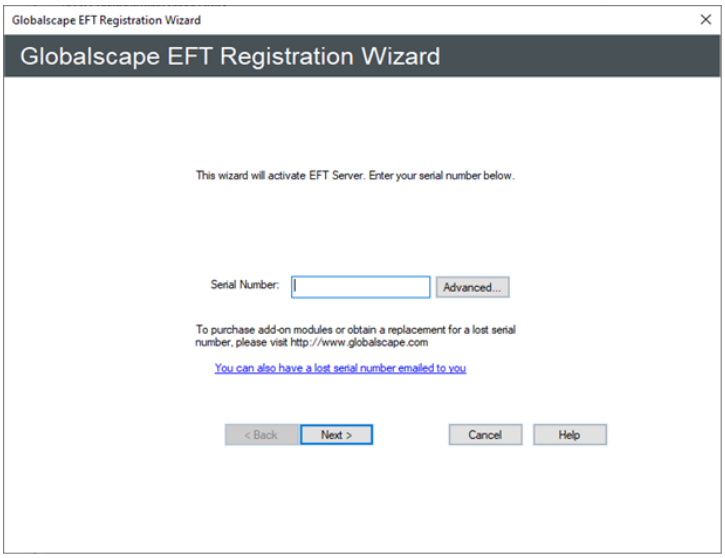
To activate online, you must be connected to the Internet, and activation must be performed through the administration interface on the EFT computer. You cannot activate through a remote installation of the administration interface.

Refer to If you do not have Internet access on the EFT computer for manual registration without the Internet.

After you activate a product, the "Activate" text for that product on the **Help**menu is unavailable.

To activate EFT and/or add-on modules via the Internet

1. On the main menu click **Help**, and then click the product you want to activate. The **Registration Wizard**appears.



2. In the **Serial Number**box, provide your serial number, and then click **Next**.

See below for Advanced Registration Options, if needed. The Advanced Registration Options are not required for successful registration, but is for specific use cases with manual registration, or to determine if the registration server is returning a registration limit error. (A DMZ Gateway Multi-Site license requires manual registration.)

3. You should receive a message confirming online activation. Click **OK**. Activation is complete. (If registration fails, try entering your serial number again.)
4. The **Help > About**dialog box displays the status of the activation, such as number of licenses on certain modules, and whether it is a standard or subscription license, and renewal date.
5. Once you've activated module, the text on the **Help** drop-down menu will dim to indicate that it's registered, aside from the **Activate Workspaces Module** text which does not dim, because you can add more seats, as needed.

Subscription Licenses:

IMPORTANT: EFT reaches out to the server at **dbregistration.globalscape.com** on port 80 to send the registration request, and receive the registration response back. If EFT cannot connect directly, it will attempt to connect via each DMZ Gateway defined (as a proxy) in turn. If that still fails, please contact Support.

- A subscription license key can be used to activate EFT and modules.
- Click **Help > Activate**[product name], and follow the prompts to active your license(s).
- The **Help > About**dialog box displays the subscription license type and the subscription term, which is based on the term dates stated in your invoice.
- Upon the renewal date, EFT will attempt to re-activate the license and, therefore, must have internet access at that time.
    - If there are additional months/years remaining in your term, EFT will successfully renew and start its countdown to the next renewal date.
    - If your subscription has run out or if EFT encounters any other problem during renewal, EFT will enter a grace period. This grace period affords you the time to contact sales and renew your subscription, if desired.

      During the grace period, EFT will attempt to renew the subscription every hour, if possible, for about a week, before it finally gives up or succeeds. While it attempts to renew, EFT will display warnings upon administrator login, and will log an event to the Windows Event Log. If it succeeds, then the new renewal date is shown in the **Help > About** dialog box. If it fails,

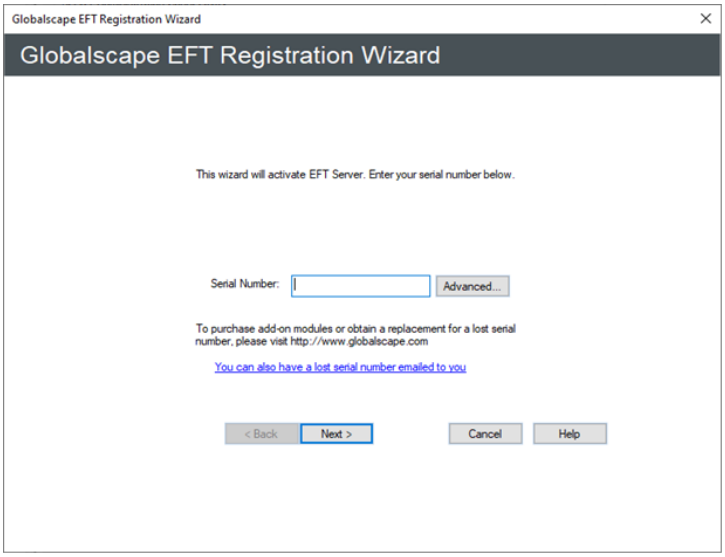
then EFT will enter its pre-activation state, where all modules become disabled and all protocol activity will cease.

After the grace period runs out (1 week after expiration of subscription), you must deregister and then reregister (activate) the licenses (assuming we have received payment).

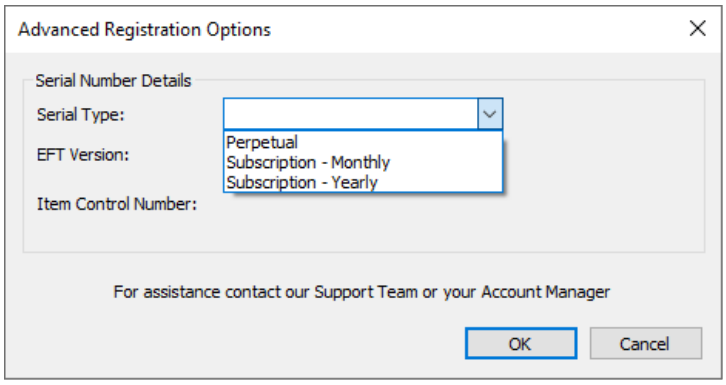
The Advanced EFT Registration options allow EFT administrators to provide more details on a registration request so that they can obtain proper registration status or correct manual registration details. When the Advanced Registration Options is configured and submitted to the registration server, EFT will make one single request to the Registration Server with the defined **Item Control Number** (IcN) instead of trying multiple attempts to register EFT or the corresponding module.

To register a subscription license

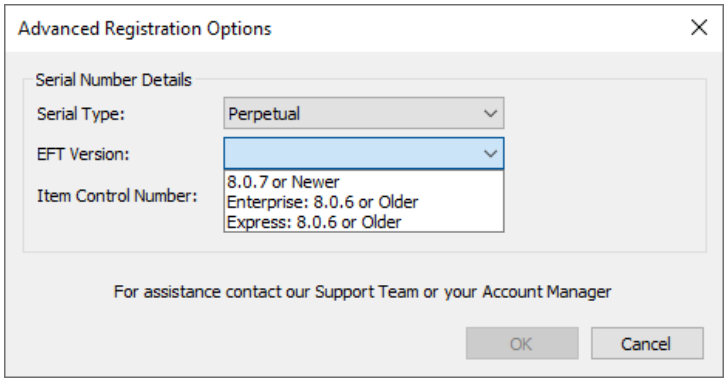
1. In the administration interface, connect to EFT then click the **Administration** tab.
2. On the main menu, click Help > then click the product that you want to register.



3. Next to the **Serial Number** box, click **Advanced**. The **Advanced Registration Options** dialog box configures specific serial number details that are then sent to the registration server.
4. In the **Serial Type** box, click the drop-down list and click the type of serial number: **Perpetual**, **Subscription - Monthly**, or **Subscription - Yearly**.



5. In the **EFT Version** box, click the drop-down list and click the version number you are registering.



   The **Item Control Number** (IcN) box is a read-only field which is populated with the IcN (item control number) of the given configuration. This information is provided in case the customer needs to reach out to Support.

Additional notes:

- The Advanced Registration Options are retained only for the current registration session. If you close the Registration Wizard or successfully register a module on any subsequent attempts, the previous configuration is not retained, and the EFT admin must reconfigure the Advanced registration details.
- If you want to undo the configuration, you need to close the Registration Wizard and relaunch the module registration to try again.
- Advanced Registration Options are not submitted on the registration request unless you make modifications to the Advanced Registration Options and click **OK**.
- Making changes and clicking **Cancel** will not submit the advanced registration options, and existing behavior is submitted to the registration server.

- When configured, and **OK** is clicked, the registration request will submit the configured IcN that is displayed in Advanced Registration Options along with the entered serial number.
- Only one request is made to the registration server instead of multiple requests; the IcN that is displayed in the Advanced Registration Options along with the entered serial number are submitted.

If you do not have Internet access on the EFT computer:

1. Complete registration information in the Registration Wizard, as usual:
    - Serial number
    - Registered to information on next page
2. Click the option to email registration request.
    - Ignore any message that says "could not find mail software." This action is to copy information into the clipboard.
3. Open up a text editor.
4. Paste the content from the Clipboard into the new blank text document.
    - The first line should say something about emailing; delete that line.
5. Save this document and transfer it to a computer that has Internet access.
6. Copy the information from the text document and paste it into the form found at this address: http://www.sat.globalscape.com/register/.
7. Click **Register Me**.
8. This will either download a REG file or output the information within the browser, depending on the browser that you use.
    - If it is in the browser, copy this and paste it into a new blank text document. Save it as a .REG file and move it back to the server computer.
9. With the service NOT running, double-click the REG file to merge the key to the registry.
10. Restart the EFT server service. When you log in to the administration interface, you should see that it is registered when you click **Help > About**.
11. Repeat these steps for any additional modules that need to be registered.

Alternatively, you can email the content of the Clipboard to `manreg@globalscape.com`. You will receive a .REG file from Globalscape Support.

Windows Account for the EFT Server Service

After it is installed, EFT has access to local folders and files. To run EFT as a service with permissions to the network and mapped drives, you must create a Windows account, set Windows NT permissions for EFT, assign the EFT server service to the account, and log EFT on as a service. Security policies should allow user accounts to log in locally.

- Create a Windows account
- Set Windows NT permissions for EFT
- Assign the EFT server service to the account

The EFT server service must have full administrative rights to:

- the folder in which you install EFT
- the location in which the users' home folders are stored
- the Windows Registry
- map a virtual folder to a network drive

With administrative rights, the service can save all of your settings. ***If the service does not have administrative rights***, you will lose settings and user accounts whenever you restart the EFT server service, and you will need to reset permissions on the computer on which the EFT server service is running.

If EFT is running in HA mode and sharing a network resource, you must run the EFT server service with an account that can access that shared network resource.

> **NOTE:** During upgrade, the name of the server service could be different, depending on the version you upgraded from; therefore, you will lose the connection to the server service Log On account. Refer to Assigning the Service to a Windows User Account to add the "Log on as" account for the EFT Server service.

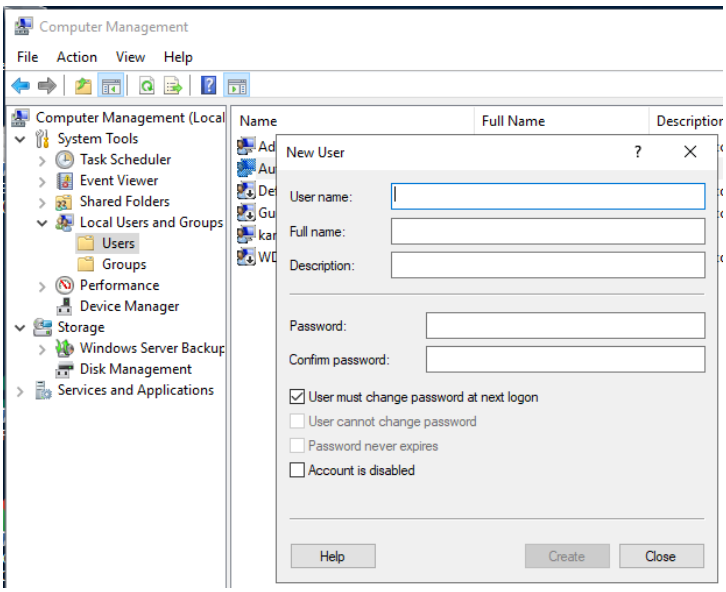
Refer to Local Security Policy Setting when Using Active Directory Authenticationfor more information about configuring EFT on an AD network. Consult with your AD network administrator for assistance, if necessary.

After you have installed EFT, created a Windows account for EFT, and assigned permissions to the account, you should edit the service itself so that it will ***not***run as a "System Account" (the default account choice). Running the service as System Account poses the potential hazard of giving users complete access to your system.

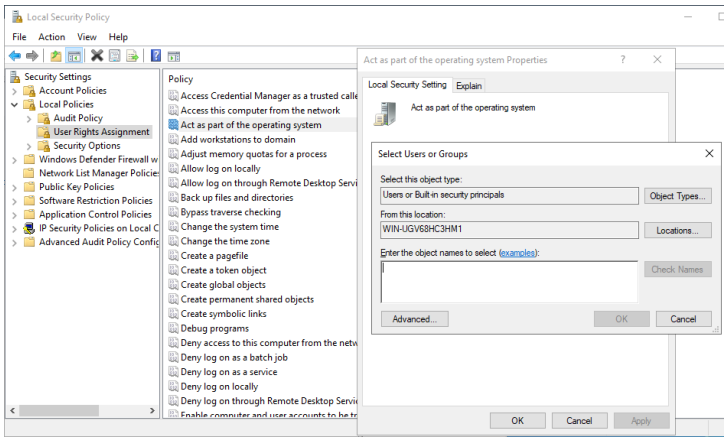
Creating a Windows User Account for EFT

To create a user account in Windows

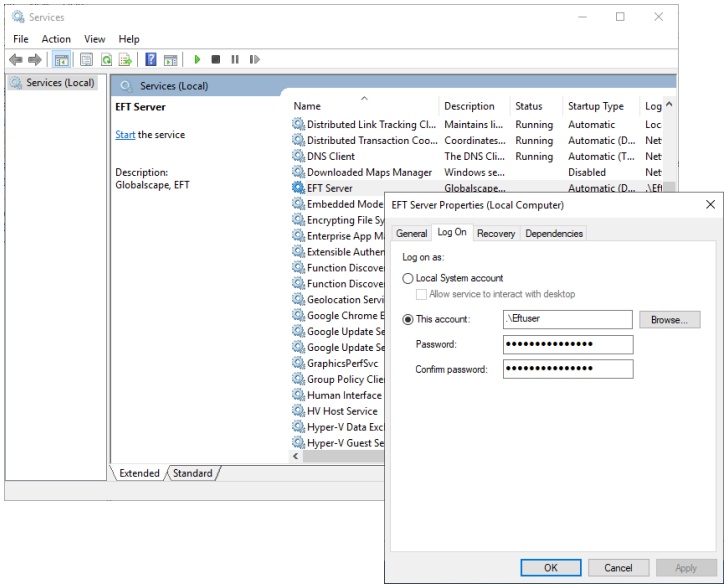
1. After you install EFT, open the Computer Management console. (In the Windows **Search** box, type `computer management`.)
2. Expand the **Local users and Groups** node, right-click **Users**, then click **New User**. The **New User** dialog box appears.



3. Create a user account for EFT (for example, EFTUser), clear the **User must change password at next logon** check box, and then click **Create**, and then click **Close**.
4. Close the Computer Management console.
5. Open the **Local Security Policy** console. (In the Windows **Search** box, type `local security policy`.)
6. Expand the **Local Policies** node, and then click **User Rights Assignment**.
7. In the right pane, in the **Policy**column, double-click **Act as part of the operating system**. The **Properties**dialog box appears.
8. Click **Add user or Group**. The **Select Users or Groups** dialog box appears.



9. Select the new user you just added (for example, EFTServer), click **Add**, then click **OK**.
10. If necessary, assign permissions for this user account in Windows.
11. Assign EFT to the new user account and log EFT on as a service.



Set Windows NT Permissions for EFT

After you have created a new Windows user account for EFT, use Windows' permissions to set the permissions for folders, files, or drives for the account. Permissions should be as restrictive as possible while still allowing EFT enough permission to run.

Using Windows NT's permissions, set the permissions for files or drives of this user to be as restrictive as possible, while still allowing EFT to run. After carefully determining which files and network folders your users will need to access, gradually increase the permissions.

Make sure that full permissions are granted to the EFT service domain user account for the following locations:

- Installation folder
- Application data folder
- Windows Temp folder
- Any shared drive paths required by EFT
- Any output directories that EFT may need to read/write files to
- The Windows Registry

If you run into permissions issues, run Process Monitor or similar tools and isolate non-success results caused by cftpsai.exe, cftpstes.exe, gsawe.exe, and any other EFT-related processes.

Using NT Authentication, user permissions override EFT's permissions. For example, if EFT has read-only access to folder1, but user John Doe has read and write permission to folder1, John Doe has the same permission when he accesses folder1 through EFT.

Windows NT permissions can be edited through the Security tab in the Properties of a file or folder. On the **Security** tab, select **Permissions**to display and edit the permissions for the object. The appearance of this dialog box is slightly different for files and directories, but in both cases, the following permissions can be granted to users or groups:

- R (Read)
- W (Write)
- D (Delete)
- P (Edit permissions)
- O (Take ownership)

Keep in mind that you have the option to grant or withhold read and write permissions. Read-only permissions are the most secure, because they allow users to access a file, but not to change it. For example, most users will need limited read access to the Windows folders (C, WinNT); however, most FTP Servers will not need ***any*** access to these directories at all.

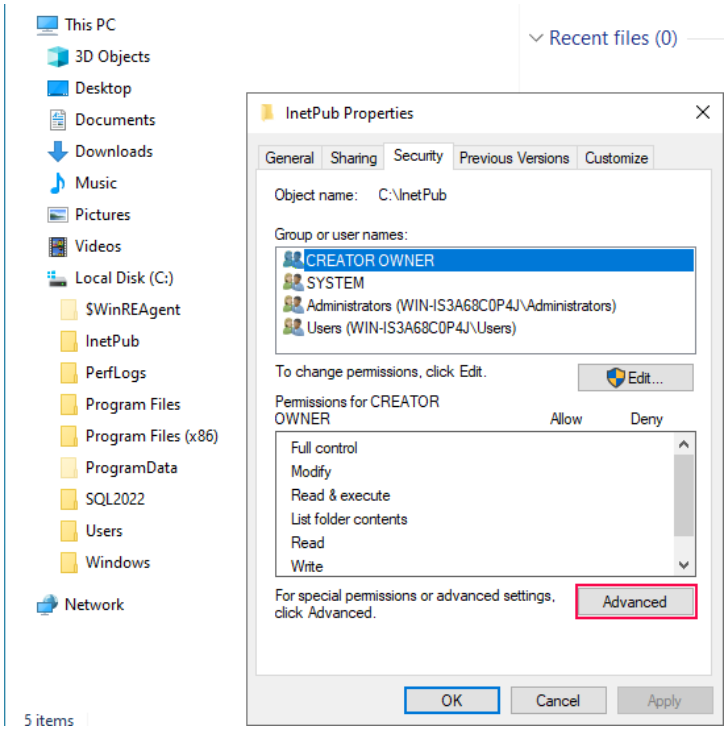
In addition to the individual permissions, Windows NT permissions also provide access levels that are pre-built sets of the existing permissions. Typically, you assign an access level to a user rather than granting individual permissions. One such access level is called "No Access," which does not contain any permissions.

To view and edit the permissions for a folder or file

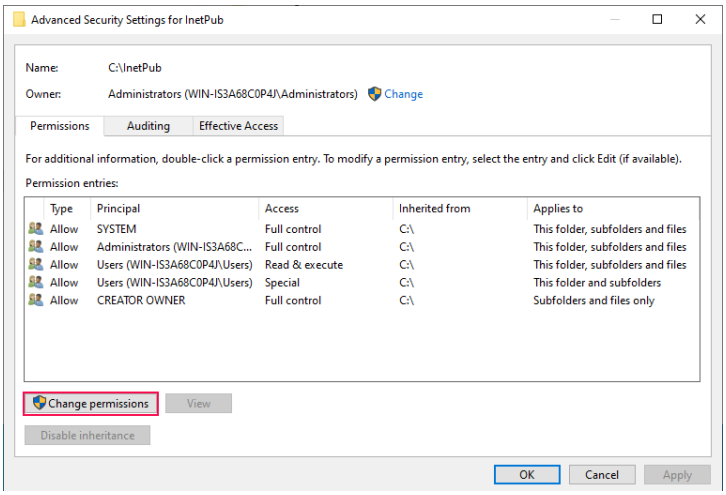
1. In Windows File Explorer, right-click the file or folder, then click **Properties**.
2. On the **Security** tab, click **Permissions**. The appearance of this dialog box is slightly different for files and directories and for different versions of Windows (W2K, XP, etc.).

Ensure that the child folders and files in EFT's \InetPub\ (C:\InetPub\) directory have the correct permissions.

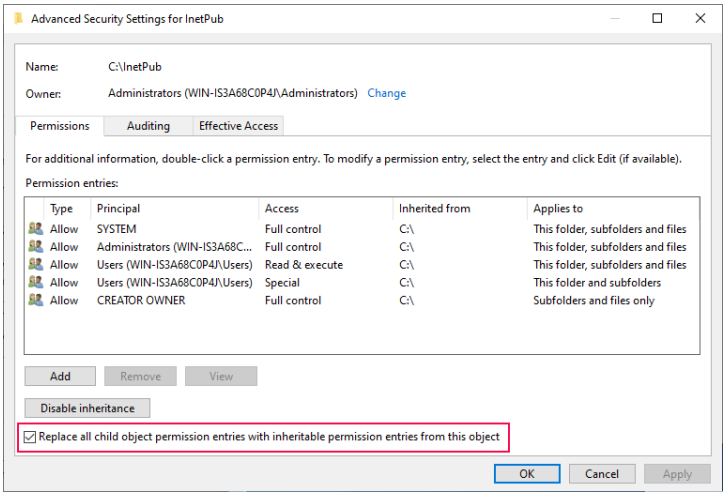
1. In Windows File Explorer, right-click the EFT user home folders directory (for example, **C:\InetPub**), then click **Properties**.



2. In the **Properties** dialog box, click the **Security** tab, then click **Advanced**. The **Advanced Security Settings** dialog box appears.



3. On the **Permissions** tab, click **Change permissions**. The dialog box will refresh.



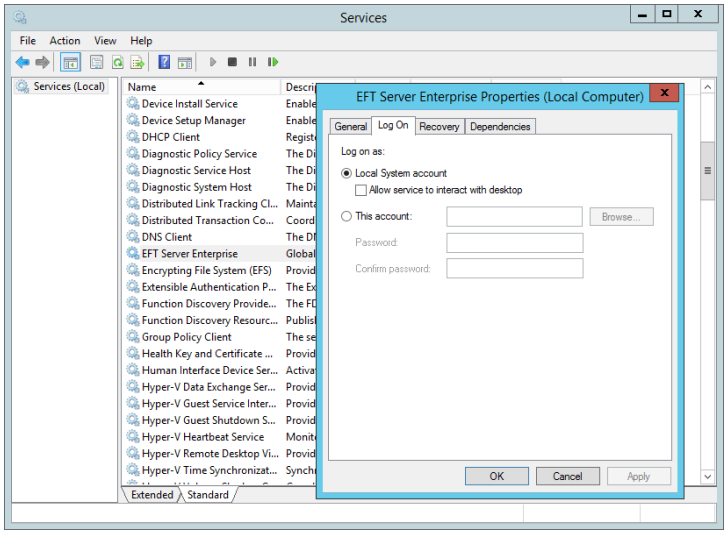
4. At the bottom of this tab, select the **Replace all child object permissions entries with inheritable permission entries from this object** check box. This will ensure that child objects will inherit the permissions of the selected object.

For more information about setting permissions to folders and files, refer to the Windows Help documentation for your specific operating system.

Assigning the Service to a Windows User Account

To assign the service to a Windows user account

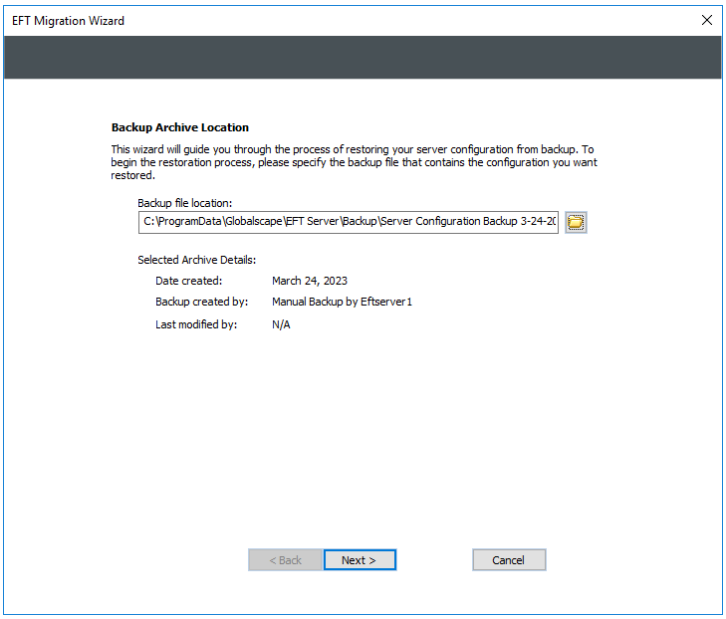
1. Click **Start > Run**, type `services.msc`, then press ENTER.
2. In the **Services** console, right-click the EFT server service, and then click **Properties**.
3. Click the **Log On**tab, then click **This account**.



4. Provide the proper credentials, then click **OK**.
5. Restart the server service.

Backing Up or Restoring Server Configuration

When migrating from a development, staging, or test computer to another computer, you cannot simply copy over EFT's configuration files to the new host. You can use the EFT Migration Wizard (pictured below) to gather each of the necessary files, then package them into one easy-to-transport file. The Migration wizard can recreate the entire folder structure and settings automatically or you can run it in manual mode and verify every setting as you step through the wizard. (Physical folders under the VFS are not recreated when the configuration is restored. However, if those physical folders are present at the time of restoration, then any VFS permissions assigned to the folders are retained.)



The EFT Migration Wizard is an interactive tool designed to assist you in the following situations:

- **Performing Disaster Recovery**. If the production Site is corrupted and configuration is lost, damaged, or destroyed, the wizard can assist you with restoring EFT to a prior working state.
- **Migrating from staging to production or to new hardware**. If you want to move EFT from a staging or development box to a production server or have set up a Server with one or more Sites on one computer and want to move it to another computer or a different network location, the wizard can assist you with gathering all the necessary files for a successful move.

  - If you are migrating from a test environment to a production environment and do not need to keep the test environment's Server, Site, and user configuration settings, you do not need to use the EFT Migration Wizard. You can just start from scratch, and run the Server, Site, and New User wizards on the new system.
  - The migration wizard will only accept **backups created with the same version** that is being restored to; using backups from different versions will not work.
  - To restore, you will use the login credentials of the server administrator that you are logged in as, regardless of the credentials used to back up the configuration.
- **Backing up for disaster mitigation (routine backups, or backup prior to major changes)**. If you need a backup to be readily available and require automatic backup, the wizard can backup all of your settings. The EFT Migration Wizard can also help if a major change is about to be made, such as new hardware changes to the EFT computer, and you need a mechanism to manually backup the current configuration. The EFT Migration Wizard can take a snapshot immediately before the major change takes place, in addition to the automatic daily backups.

The migration fails if there is a mismatch/discrepancy in listening IP addresses, VFS root or structure, Authentication Manager settings, DMZ Gateway settings, or database connectivity.

The Migration wizard backs up the entire EFT configuration in an archive file at a path that is accessible to the EFT service.

Log files are not backed up in the Backup and Cleanup Rule (because that is intended as a configuration backup). You can create your own Event Rule to back up log files, if needed.

The following items are backed up to C:\ProgramData\Globalscape\EFT Server\Backup (by default):

- The configuration files
- All certificates and keys that are pointed to from configuration files
- Any custom reports
- Advanced properties
- The \Web\ folder to capture any customizations
- Entire VFS structure (physical folders recreated only under the Site root, not those pointed to by virtual folders)
- Any Advanced Workflows created

The wizard can be initiated manually in the EFT administration interface from the **File** menu or automatically in Event Rules. When you create your first Site, a Timer Rule is created that runs the **Backup Server Configuration** Action once a day at midnight, using all defaults for naming and backup location (**\backup\Server Configuration Backup [Month] [Day] [Year].bak**). The Rule includes a **Cleanup** Action to delete backup files (***.bak**) older than 30 days in that same folder. This **Backup and Cleanup** Rule is enabled by default, but you can disable it and edit it as necessary.

It is a good idea to save the backup on a drive other than on the one on which the EFT is installed. If EFT's hard drive fails, you will want to use the backup to restore configuration. Refer to Backup Server Configuration Action for details of editing the **Backup and Cleanup** Rule.

To manually back up Server configuration

1. On the main menu, click **File > Backup Server Configuration**. The standard **Save As** dialog box for your operating system appears.
2. Specify the location in which to save the backup, then click **Open**. Save the backup on a drive other than on the one on which the EFT is installed. The configuration is saved and is named *Server Configuration Backup [Month] [Day] [Year]* with a **.bak**extension.
3. One of the following occurs:
    - If a "backup successful" message appears, click **OK**to dismiss the message.
    - If a failure message appears, restart the EFT service, then run the backup again.

Any configuration changes made since the backup are, obviously, not included in the restore. For example, if you have deleted or added users since the last backup, those users will have to be deleted or added again after you restore.

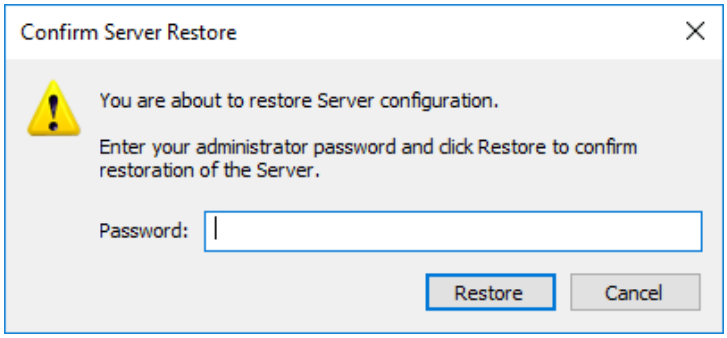
Backups from IPv4-only EFT versions will listen only on IPv4 addresses; if all listeners selected for administrative connections are unavailable, then switch to listening on localhost.

To restore Server configuration

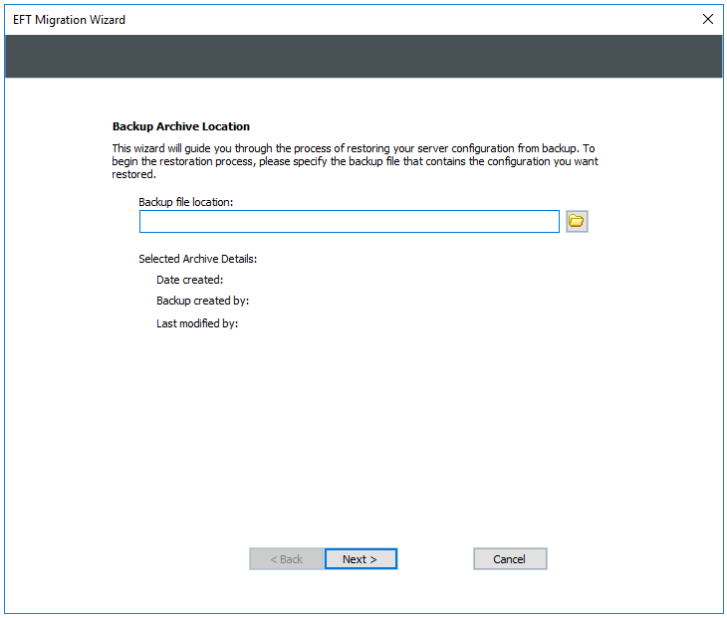
1. Install and activate the product on the target system, if restoring to a different computer.
2. After installation is complete, the **New Administrator Connection** wizard appears. You must configure the local connection (that is, create the LocalHost Server object in the tree) before you can restore from backup.

3. In the **Connection**wizard, leave **This computer**selected, and specify the **Label** for the local connection. By default, the label is `LocalHost`. Because LocalHost is a very common label, it is a good idea to change the label to something that is easily identifiable in error logs, reports, and remote connections. For example, `GS_EFTS`. You can label EFT anything you want; the EFT name is ***not*** dependent upon the computer name.
4. After you are logged in to EFT, do one of the following:
   - In the **Server Setup** wizard, click **Restore from Backup**.
   - On the main menu, click **File > Restore Server Configuration**.

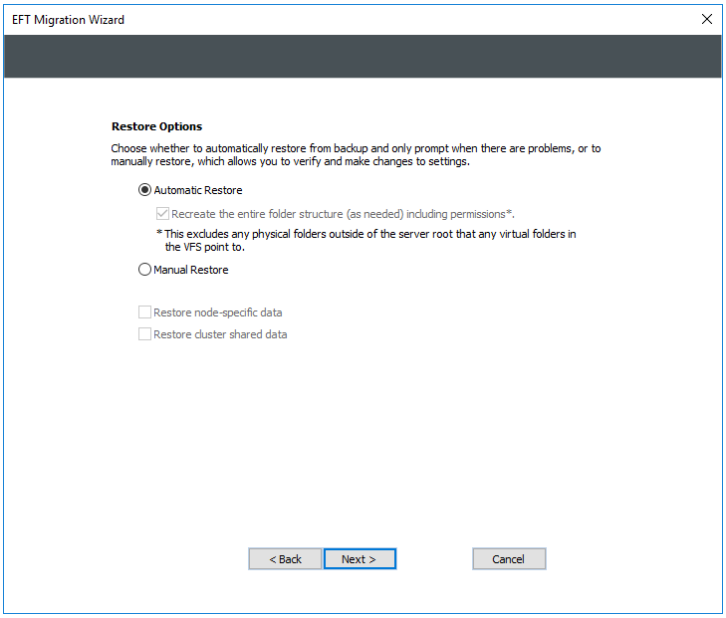
   The **Confirm Server Restore** dialog box appears.



5. Provide the administrator login credentials for the configuration being restored, and then click **Restore**. (You can use the EFT administrator credentials, Windows Authentication, or the currently logged on user's credentials.) The **EFT Migration Wizard** appears.



6. Select the folder icon to select the backup to restore. The path to the backup file appears in the **Backup file location** box. The **Selected Archive Details** area displays the date the backup was made and the username that created the backup, if it was a manual backup, or "Automatic Recurring Backup" if it was an Event Rule-created backup.
7. Click **Next**. The **Restore Options** page appears.



8. Select the **Restore node-specific data** check box to restore data that is specific to that node (that is, listening IP address, DMZ Gateway settings, registration).
9. Select the **Restore cluster-shared data** check box to restore data that is shared amongst the cluster. When this check box is selected, the **Recreate the entire folder structure** check box is also selected. Clear that check box if you do not want to recreate the folder structure.

   When the restore process begins, other nodes stop with -1 error. This triggers them to be restarted by Windows Service Manager, at which point those other nodes will wait for restore operation to complete. Once the restore has completed on one of the nodes, the other nodes that had been waiting will proceed with loading configuration. After the restore completes, the node that did restore also restarts in the same way. Thus, all nodes in the cluster have restarted with restored configuration up-and-running.

10. Click either **Automatic Restore** or **Manual Restore**:

    Automatic Restore—Automatic Restore prompts only when the wizard encounters discrepancies or problems with restoring. **Automatic Restore** is the default setting. In automatic mode, you are not prompted to verify settings or allowed to change them.

    a. Click **Automatic Restore**. The **Recreate the entire folder structure** check box is selected by default. Clear this check box if you do not want to recreate the VFS folder structure.

       If your EFT folder structure includes user folders (for example, C:\Inetpub\EFTRoot\MySite\Usr\<username>), if you clear the **Recreate the entire folder structure** check box and do not recreate these folders manually, the users will not be able to access their folders.

    b. Click **Next**. The **Ready to Restore** page appears. Read the information on the page, and then click **Restore**.
    c. After the Server is restored, restart EFT and log in to the administration interface. A log appears describing the restore process, including file names and paths, and contains any errors encountered during restore.

    Manual Restore—Manual Restore allows you to verify and make changes to settings, as needed.

    a. Click **Manual Restore**, and then click **Next**.

       The **Server Administration Connectivity** page appears.
    b. Review the IP address for each Site. If you are restoring a Site to a different IP address, click to edit the IP address in the **New IP Address Assignment** list. The **Sites to Restore** page appears.
    c. Click **Next**. Select the check boxes of the Sites whose settings you want to import and clear the check boxes of the Sites whose settings you do not want to import.
    d. Click **Next**. In the **Site Listening IP Address Assignment** page appears. Click the links to specify one or more IP addresses to use (or All Incoming), and then click **OK**.
    e. Click **Next**. The **Site Authentication Manager Settings** page appears.
    f. The authentication database for each Site to be restored appears in the list. In the **Settings**column, click **View/Modify**if you want to view or change the path where EFT will store the user database. (You cannot change the type of authentication.)

- If EFT cannot connect to the Site's authentication provider, an error message appears.
- Click **OK**to continue as is or click **Cancel**to modify the authentication provider settings.

g. Click **Next**. The **Site Root Folder** page appears.
h. Review the root folder location for each Site that you are restoring. If necessary, click the folder icon to specify a different location, and then click **Next**.
i. If the DMZ Gateway is defined and configured in EFT that you are restoring, the **DMZ Gateway** page appears. If not, skip this step.
    i. Review the IP addresses and ports for the DMZ Gateway. Click to edit the IP address or port, if different.
    ii. Click **Next**. EFT will test the DMZ Gateway connection and, if successful, the wizard proceeds to the next page.
    - If a failure occurs, the wizard displays a warning prompt indicating failure to connect to the DMZ Gateway and allowing you to either fix the problem (go back to the previous page to verify the IP address and port) or proceed anyway (if the IP address and port are correct, but the DMZ is not communicating).

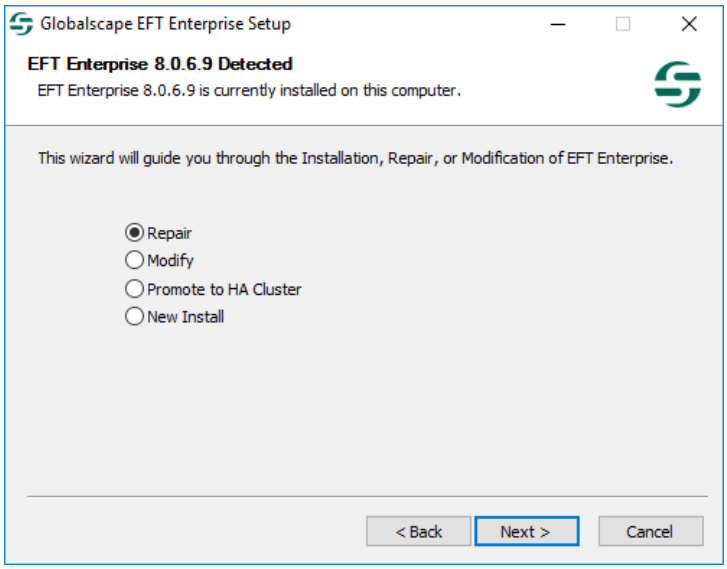
j. If the Auditing and Reporting module is defined and configured in EFT that you are restoring, the **Auditing Database Connectivity** page appears. If not, skip this step.
    - Click **Test**to verify connectivity to Auditing and Reporting Module queue and, if successful, send a test message to the database. If a connection to the database cannot be made within 5 seconds, a warning prompt appears. (Verify that the database is available.)

k. Click **Next**. Database connectivity is again verified and the **Ready to Restore** page appears.
l. Read the information on the page, and then click **Restore**.
m. A message appears indicating whether the configuration was successfully restored. Click **OK**.
n. Review the log if errors were encountered during restore.

Modifying or Repairing the Installation

After you have installed EFT, you might later want to install other features, such as the administration interface or the Auditing and Reporting module. Or, if you accidentally deleted or edited necessary program files, you can repair the installation.

If you want to promote a stand-alone EFT server to an HA node, use the **Modify** option.



To modify or repair the software

1. Launch the installer. The installer will detect an existing installation.
2. Do one of the following:
   - To upgrade the existing installation, click **Repair**. (**Repair** overwrites changed files and reinstalls missing files.)
   - To install or uninstall specific components, click **Modify**. (**Modify**installs selected components; removes unselected components.)
   - To install a fresh installation, including a new configuration file, click **New Install**.
3. Click **Next** and follow the instructions in the wizard. Refer to Installing EFT, administrator, and Modules, if necessary.
4. If you chose **Modify**in step 2, on the **Components**page, select the check boxes of components you want to install and clear the check boxes of components you want to remove. ***If you clear the check box of an installed component, it will be uninstalled!***

5. When the wizard is finished, restart the Server services. The EFT service **Log On as** account will be set to **Local System** account by default. You can edit this in the service's **Properties**dialog box, on the **Log on**tab. (**Start > Run >**`services.msc`.)

Repair/modify activities are logged in the installer log file (for example, **C:\Program Files\GlobalSCAPE\EFT Server**). If you need additional information or help, visit Globalscape's Support Center.

Promoting EFT Stand-Alone to Cluster Node

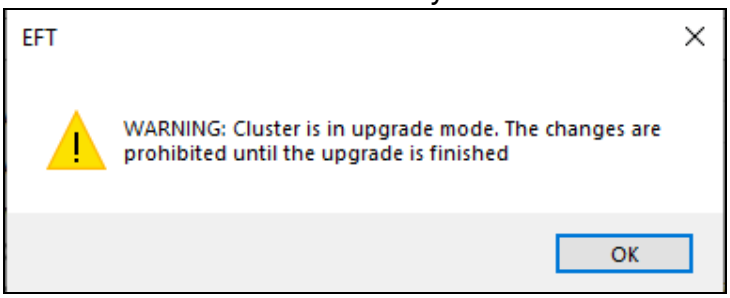
You can "promote" an EFT stand-alone server to a new cluster node. Refer to Globalscape Knowledgebase article #11542, Promote Stand-alone EFT to HA node for details of promoting a stand-alone server to a node in a cluster configuration.

You cannot promote a stand-alone server to an existing cluster. In that case, you would have to reinstall EFT on the stand-alone box as a active-active server, using instructions in Upgrade HA Nodes with Zero Downtime, and then point the new active-active server to the existing cluster configuration path.

Upgrade HA Nodes with Zero Downtime

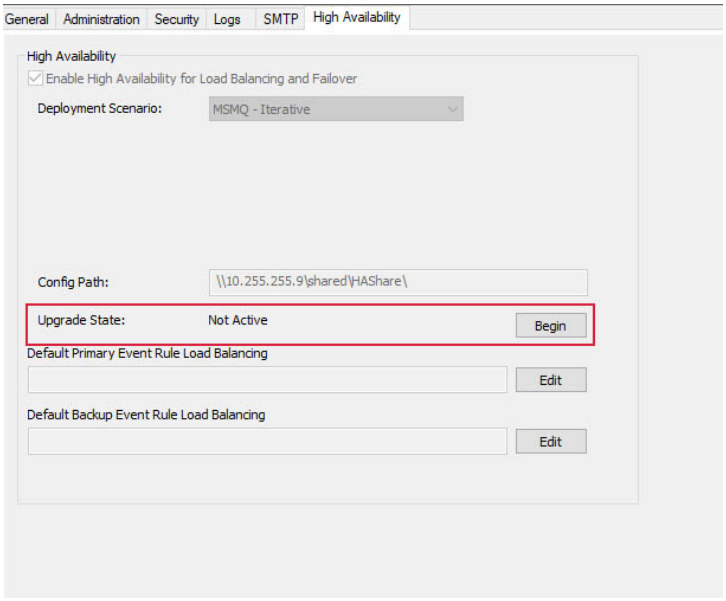
EFT administrators can upgrade their HA nodes with "zero downtime," meaning you can upgrade a cluster without stopping all nodes at the same time.

NOTE: The warning prompt "Cluster is in upgrade mode" is thrown when a user makes a configuration change and then refreshes the EFT administration interface while the server is in "read only" mode.



The Server > HA tab is used to manage the cluster upgrade state

- The button will be displayed as **Begin** when upgrades have not been started.



- The button will be displayed as **End** when upgrades have been completed. Administrators can execute the End state at any point, but nodes that have not been upgraded will fail to start until they are upgraded.
- When enabling the upgrade, EFT administrators will be prompted with a warning

that the transition and change cannot be undone.

- The warning prompt should reference details to review documentation.

To upgrade all of the HA nodes at that same time—without stopping any nodes

In the EFT administration interface, on the **Server > High Availability** tab, you must manually put the cluster into the **Upgrade** state, upgrade each node one by one, then after the upgrade has completed successfully, manually transition the cluster back to **Normal** state.

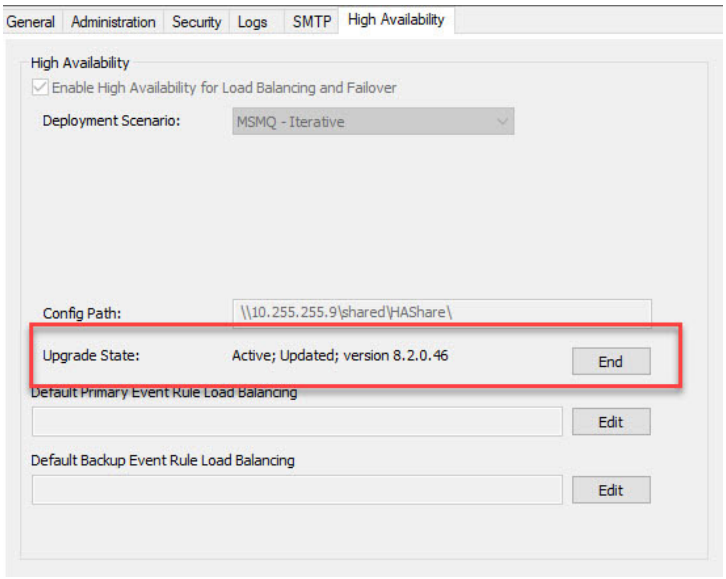
- **Upgrade State**. Allows simultaneous updates to nodes that have an **Outdated** version.

  Upgrade state limitations:

  - Backup/Restore feature is prohibited
  - No configuration changes are allowed during the Upgrade state, except moving the cluster back into the Normal state
- **Normal State**. Requires all nodes have the same version. Upon transition to Normal, the Upgrade State will display “Not Active”

  Normal state limitations:

  - Loading old nodes is prohibited. EFT will not start when the nodes are not upgraded.
  - You will be unable to transition from Upgrade to Normal when an upgrade has not been completed. This only affects nodes that have not been upgraded.
  - EFT will prevent COM API from transitioning from Upgrade to Normal state. A proper response code/error will be presented
  - EFT will prevent REST API from transitioning EFT from Upgrade to Normal state. A proper response code/error will be presented.
  - When upgrade has ended (at the global level or a node that was upgraded), for any nodes that were not upgraded, the EFT Server Service will stop and fail to start until they are upgraded.
  - Transition state from Upgrade to Normal are global, which affects all nodes within the cluster, so administrators should only end upgrades after all nodes have been upgraded.



Upon successful HA upgrade to a new version, the **High Availability** tab's **Upgrade State** will display “Active; Updated; x.x.x.x”, where x.x.x.x is the newer version of EFT (the version to which EFT was upgraded).

Normal state to Upgrade state

- All nodes are Outdated. Admin logins to any of the nodes and enter the cluster into the "Upgrade" state (with GUI/COM/REST).
    - EFT admins shall be able to transition from Normal to the Upgrade state via our EFT administrator interface High Availability tab.
    - EFT admins shall be able to transition from Normal to the Upgrade state via COM. Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade.
    - EFT admins shall be able to transition from Normal to the Upgrade state via REST API. Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade.
    - The ability to start the Upgrade state is a global setting; once set at any node, all nodes will report the same state.
    - Upgrade state should be used ONLY when upgrading to a new version of EFT and not when an EFT administrator forgets to upgrade a node in the cluster from a previous upgrade.
- Once configured for Upgrade, the cluster is in Upgrade state, and you can upgrade each node one by one.

- Outdated nodes write audit data to local *.sql files only; Each node will have their own local *.sql file.
- Updated nodes write into ARM database; If no SQL schema changes exist, there is a post process in the Normal state that will migrate the data from the *.sql file into the ARM database.
- Uses Web folder appropriate to node's version.
    - The nodes' version should match the same version.
    - Shadowfax folder will be copied from \\<HASharedPath>\Web to \\<HASharedPath>\UpgradeFromx.x.xx (where x.x.x.x is the older EFT version); This …\UpgradeFromx.x.x.x will be used for Outdated nodes.
    - Shadowfax folder \\<HASharedPath>\Web will be used for Updated nodes and will be updated with the first upgraded node.
- Outdated nodes allow admins to login in read-only mode. EFT administrators will not be able to make any configuration changes to EFT.
- Updated nodes allow admins to login in read-only mode AND move the cluster to Normal state.
- Configuration changes write in deltas only (there could be only internode mx messages).
    - Changes are not saved into the configuration files, ServerConfig.db and SiteConfigXX.db files. (Part of the advanced property HAFullConfigDumpIntervalMins.)
    - Internode mx messages are communications between EFT nodes (no QA validation).
- Unknown internode messages are ignored; These are internal nodes for Outdated nodes that may not know about freshly added internode messages in Updated nodes.
- Cluster Management subsystem doesn't send any messages and ignores all received messages.
- ERLB subsystem doesn't delegate to run any event rules - all rules are processed with Master node only. Client connections to the server will be processed without any restrictions during the Upgrade state.

Upgrade state to Normal state

- All nodes are Updated. Admin will need to log into any node and end the upgrade which will switch it back to Normal state (with GUI/COM/REST)

    - EFT admins shall be able to transition from Upgrade to Normal state via our EFT Admin UI
    - EFT admins shall be able to transition from Upgrade to Normal state via COM; Appropriate error message(s) will be provided if enabling Normal state on any node when the cluster is already configured for Normal
    - EFT admins shall be able to transition from Upgrade to Normal state via REST API; Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade
    - The ability to end the upgrade state is a global setting; once set at any node, all nodes will report the same state. Nodes that were not upgraded and the upgrade state has ended, will fail to start.
    - Nodes that were not upgraded after the Upgrade state ends, now Normal, can be upgraded later and will be visible and continue to work in the cluster
- Normal state limitations: Loading old nodes is prohibited. EFT will not start when the nodes are not upgraded

COM has several methods to manage cluster upgrade state

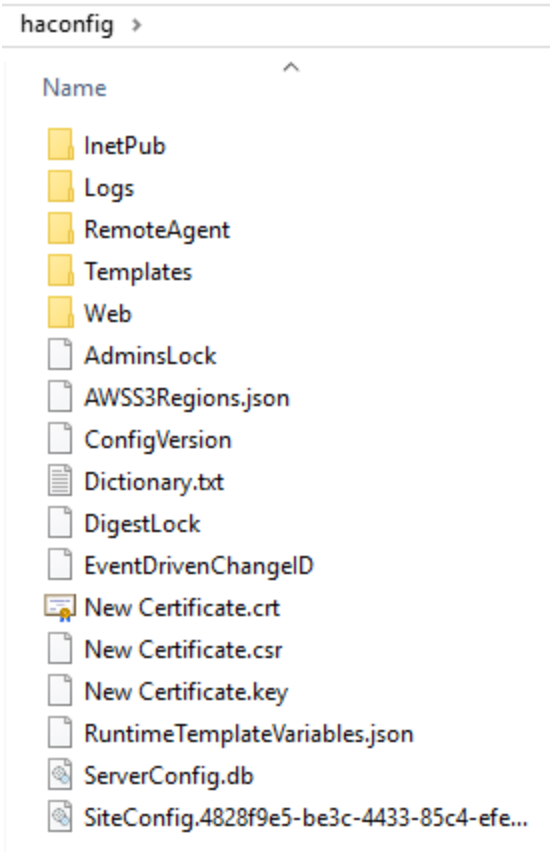
- Enum: HAUpgradeNodeState
    - NotInUpgrade = 0,
    - OldNode,
    - NewNode
- Method: ICIServer::GetHAUpgradeNodeState; Retrieves node upgrade state
- REST has two endpoints to manage cluster upgrade state:
    - Get HA node upgrade state; GET /server/ha/upgrade
    - Changes entire HA cluster state to the upgrade or normal state: POST /server/ha/upgrade

Related Topics

- Active-Active HA Cluster Installing or Upgrading the Server
- HA FAQ
- High Availability Tab of a Server

HA Nodes Configuration Files

When installing EFT in an HA configuration, you must specify a shared configuration location (which must be accessible by all of the nodes in the HA cluster). The files that all of the HA nodes will share are saved and updated in the shared configuration directory.



- An Advanced Property was added to improve performance when configuration is copied to the cluster share. When off, `HAFullConfigDumpIntervalMins = 0` or is not defined, the full configuration is copied on each change. Add the Advanced Property and set it between 1-10 minute intervals to reduce network traffic.
- A local configuration path for each node must also be specified for each node for local caching. When configuration changes are made to SSH, trusted SSL certificates, OpenPGP key materials, and AML files (Advanced Workflow tasks), those files are cached locally, and uploads are safely synchronized to the shared config path.

The other nodes then update their local cache from the central location. Thus, the central share always contains the current version of those files. When, for example, a new SSL Cert or AML file is created, the creator directly adds/modifies the files on the network share then tells the other nodes that the file was modified/created and they need to update their local cache (that is, copy the file to their local ProgramData directory).

- When using HA, **you need to specify a unique location (local) for the log files**. This is for troubleshooting purposes (to know on which node the issue occurred). Also, having two nodes write to the same file causes issues with file locking, which will cause data in the logs to be lost. For visibility into node status, enable cluster logging. Logging.cfghas new logging options specifically for HA. When configuring RSA in an HA environment be sure to have the **sdconf.rec**file stored locally for each node. Each node MUST have its own copy of sdconf.rec.
- When using Encrypted folders, you can only encrypt files in the directory hierarchy of the Site's root folder. Make sure that the Site root folder on the **Site > General** tab is pointing to the correct path. That is, if your HA config drive is on **D:\HAConfig\,** you should edit the site root folder to point to **D:\HAConfig\InetPub\EFTRoot\MySite**.

Related Topics

- Logging for HA Nodes
- HA FAQ

Administration Interface

The topics below describe the administration interface.

- Introduction to the Administration Interface
- Main Menu and Toolbar
- Server Tab
- General Tab of a Server
- Administration Tab of a Server
- Security Tab of a Server
- Logs Tab of a Server
- SMTP Tab of a Server
- High Availability Tab of a Server
- Automate Service Account
- Report Tab
- VFS Tab
- Status Tab
- Status Bar
- Administration Interface Session Timeout
- Closing the Administration Interface

The EFT Administration Interface

The administration interface of EFT is used to configure one or more physical servers and their connections. Each physical server can have one or more virtual hosts called "Sites" listening on one or more IP addresses. User accounts are attached to a Site, along with settings that can be configured via the administration interface. After you install EFT and you launch the administration interface, you are prompted to connect to EFT on either a local or a remote computer. You can install the interface on as many computers as you like, but the server service may only be installed on a computer with a valid EFT software license.

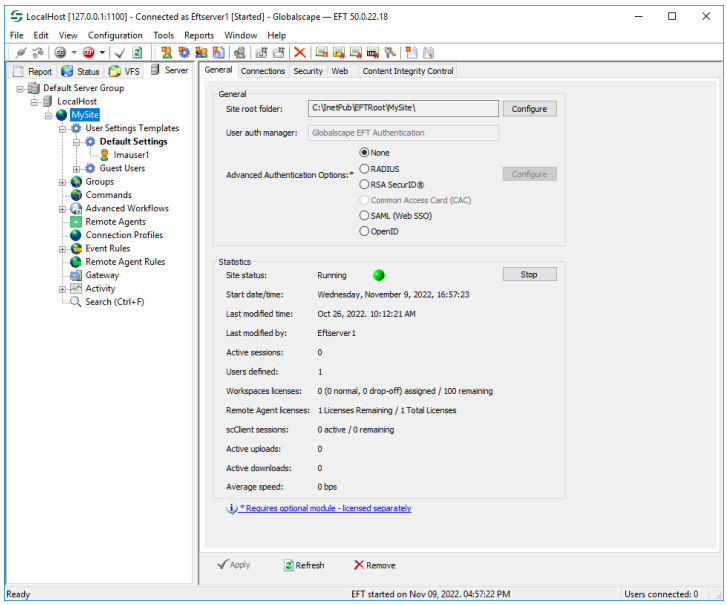
You can login as an administrator using preconfigured accounts created in the internal authentication database, Windows local administrator accounts, or Active Directory-based accounts. A drop-down list is provided from which you can choose **EFT Authentication**, **Currently Logged On User**, or **Windows Authentication**. The last-used authentication scheme selected is saved locally and recalled the next time the administrator logs in on that computer.

After EFT is configured, using the EFT computer's local administrator credentials, you can open the administration interface, login automatically from a command line, or using a Windows shortcut, on the EFT administrator IP address and port.

- EFT allows you to specify Active Directory accounts and local computer administrators as EFT administrators.
- Changing an administrator password, locking out an administrator account, removing an administrator account, enforcing complex passwords, password history, and password reset on an administrator account, and expiring passwords on administrator accounts apply to EFT-managed accounts only.

To open the administration interface

- Click the EFT shortcut on the **Start**menu or desktop (cftpsai.exe).



The left pane of the administration interface displays the **Server** tab by default. The **Server** tab provides a tree view of the administration interface components that are used to connect to and communicate with EFT (Server Groups, Servers, Sites, Settings Templates, Users, Permission Groups, Commands, Event Rules, and Gateway).

The **Report** tab, **Status** tab, and **VFS** tab provide other views. Items within each sub node of the Site are sorted alphabetically. That is, the User Settings Templates are sorted alphabetically, the user accounts in each Settings Template are sorted alphabetically, the Groups are sorted alphabetically, and so on.

The right pane provides the tabs that contain the configuration options for the item selected in the left pane. For example, when you select a Server in the tree on the **Server**tab, the right pane contains the configuration options for that Server.

When any node under the Server Group is selected, the Title bar displays the IP address and the connected username.

For details of each tab, the main menu, and the toolbar, refer to the topics below.

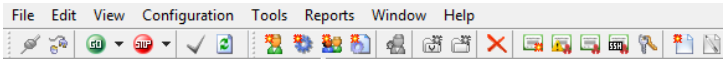
Related Topics

- Server Settings
- Report Tab
- Status Tab
- VFS Tab
- Main Menu and Toolbar
- Status Bar

- Administrator Session Timeout
- Monitoring User Connections
- Logging in to EFT

Main Menu and Toolbar

The main menu and toolbar of the administration interface provide options for configuring and managing Sites, Settings Templates, Groups, Commands, Folders, Certificates, and Reports; and for getting help, activating the server and modules, and About EFT, which displays the license details.



Below is a description of each of the main menu options and toolbar icons.

Menu Option	Sub Menu Option	Toolbar	Description
File	Connect to EFT		Opens the **Connect to EFT** dialog box in which you can log in to the selected the Server.
	Disconnect from Server		Disconnects from EFT, but leaves the administration interface open.
	Start Server Service	-	Starts the EFT service.
	Stop Server Service	-	Stops the EFT service.
	Drain Server	-	Halts NEW incoming connections and event rule activity for all sites.
	Backup Server Configuration	-	Opens a **Save As** dialog box in which you can specify a location to save a *.bak file of the current configuration.
	Restore Server Configuration	-	Opens the EFT Migration Wizard in which you specify the *.bak file to restore EFT configuration. You can only restore the same version that is backed up.
	Start All Sites		Starts all Sites on a selected EFT. Only available if one or more Sites are stopped.
	Stop All Sites		Stops all Sites on a selected EFT. Only available if one or more Sites are running.
	Start Site	-	Starts the selected Site. Only available if the Site is stopped.
	Stop Site	-	Stops the selected Site. Only available if the Site is running.
	New User		Opens the New User Creation wizard in which you can define a new user.

Menu Option	Sub Menu Option	Toolbar	Description
	New Site	-	Opens the Site Setup wizard in which you can define a new Site. The first page of the wizard provides the option of creating a standard Site or a Site created using the "strict security settings" option.
	New Server	-	Opens the **New administrator Connection**wizard in which you can create a new Server.
	New Server Group		Opens the **Create New Group** dialog box in which you can define a new Server Group.
	Kick Selected User	-	Forcibly logs off a selected user.
	Remove User	-	Deletes selected user.
	Remove Site	-	Opens a confirmation dialog box asking if you want to remove the selected Site. Also available when right-clicking a Site.
	Remove Server		Opens a confirmation dialog box asking if you want to remove the selected EFT. Also available when right-clicking the object in the tree.
	Remove Server Group	-	Removes selected Server Group; only available if you have more than one Server Group defined. (WARNING: No confirmation message appears!) Also available when right-clicking a Server.
	Exit administrator	-	Closes the administration interface. (No confirmation appears.)
Edit	Cut	-	Deletes selected text and copies it to the Clipboard.
	Copy	-	Copies selected text to the Clipboard.
	Paste	-	Pastes text from the Clipboard to a selected editable text area in the EFT administration interface.
	Server Service Settings	-	Opens the **Server Service Settings** dialog box, in which you can view the status of, start, and stop the EFT service or connect to a remote the Server service.
	Global Settings	-	Opens the **Server Global Settings** dialog box in which you can specify whether to prompt on administrator exit and Enable EFS folder icons.
View	Toolbar	-	Displays or hides the toolbar.
	Status Bar	-	Displays or hides the Status bar on the bottom of the administration interface.

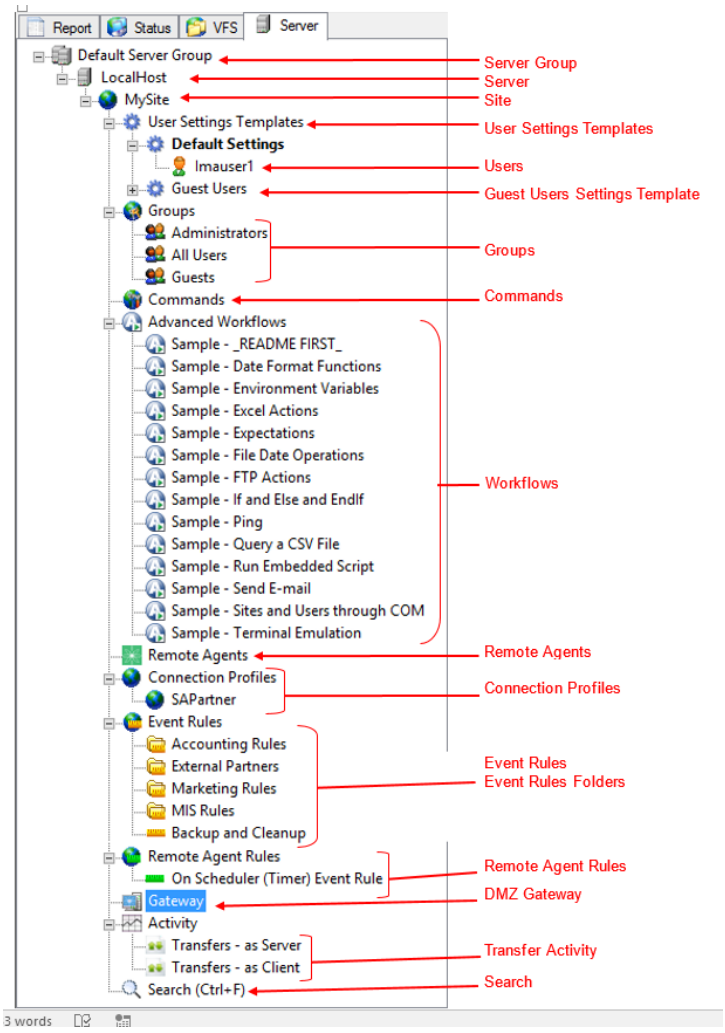
Menu Option	Sub Menu Option	Toolbar	Description
	Refresh User Database		Connects to the user database and updates EFT. For more details, refer to Configuring EFT to Automatically Update the Authentication Database and Changing the User Database Refresh Rate for a Site. The user list is not refreshed automatically when a Site is stopped for Server startup; user database synchronization timer; or administrator changes related to the user database.
	Refresh		Refreshes the display to the last saved state.
Configuration	New User		Opens the New User Creation wizard in which you can define a new user.
	New Site	-	Opens the Site Setup wizard in which you can define a new Site. The first page of the wizard provides the option of creating a standard Site or a Site created using the "strict security settings" option.
	New Server		Opens the **New administrator Connection**wizard in which you can create a new Server.
	New Settings Template		Opens the Create New Settings Template dialog box in which you can define a new Settings Template.
	New Permissions Group		Opens the Create New Group dialog box in which can define a new Permission Group.
	New Server Group		Opens the **Create New Group** dialog box in which you can define a new Server Group.
	New Command		Opens the Custom Command wizard in which you can create a custom Command for use in Event Rules.
	New Workflow Folder	-	Opens New Advanced Workflow Folder dialog box.
	New Workflow	-	Opens the Create a Workflow dialog box.
	New Connection Profile	-	Opens New Connection Profile dialog box
	New Event Rule Folder	-	Opens New Event Rule Folder dialog box
	New Event Rule	-	Opens the Create New Event Rule dialog box in which you can select an Event trigger.
	New Virtual Folder		Opens the New Virtual Folder dialog box in which you can provide a name for and create a new virtual folder.
	New Physical Folder		Opens the Create Folder dialog box in which you can provide a name for and create a new physical folder.

Menu Option	Sub Menu Option	Toolbar	Description
	Reset Subfolders	-	Available only on the **VFS** tab, used to reset all subfolders of a particular parent folder to inherit permissions from that parent.
	Rename Selected	-	Enables a selected object for renaming.
	Delete Selected		A confirmation message appears asking if you want to delete the selected object.
	Set Settings Template		Assigns the selected user to a Settings Template.
	Apply Changes		Updates EFT with any changes. (Same as clicking **Apply**.)
	Undo Changes		Reverts to the last applied change.
Tools	Create SSL Certificate		Opens the Create SSL Certificate wizard in which you can create a self-signed certificate, private key, and certificate request file (.csr).
	Sign SSL Certificate		Opens the Certificate Signing Utility in which you can sign a client's certificate request file (.csr).
	Manage SSL Certificates		Opens the Certificate Manager in which you can manage trusted and pending certificates.
	Create SSH Key Pair	-	Opens the **Create SH2 Public/Private Key pair**wizard, in which you can create a server or client key pair.
	Manage SSH Keys		Opens the **SSH Key Manager** in which you can view, rename, create, import, and delete SSH Keys.
	Create OpenPGP Keys	-	Opens the **OpenPGP Key Generation** wizard in which you can create the public and private keyring pair.
	Manage OpenPGP Keys		Opens the OpenPGP Keyring manager in which you can create, import, export, and delete OpenPGP Keyrings.
Reports	New Report		Opens the Create New Report dialog box in which you provide a name for the new report. After you click **OK**, the VSReport Designer appears in which you can define the new report.
	Edit Report		Opens the selected report in the VSReport designer for you to edit it.
	Delete Report	-	Displays a confirmation message asking you to confirm (Yes/No) whether you want to delete the selected report.
	Save Report	-	Opens the **Save As** dialog box in which you can name the report and specify where to save it. The default location is **C:\Program Files\Globalscape\EFT**.

Menu Option	Sub Menu Option	Toolbar	Description
	Import Report	-	Opens the **Open** dialog box in which you can browse for a report to import.
	Export Report	-	Opens the **Save As** dialog box in which you can name the report and specify where to save it. The default location is **C:\Program Files\Globalscape\admin\Reports**. For details of exporting reports, refer to Exporting a Report in XML Format and Exporting and Publishing a Report in the Report Designer.
	Run PCI DSS Compliance Report	-	Generates the PCI DSS Compliance Report in HTML format
	Run Data Protection Impact Assessment (DPIA) Report	-	Generates the DPIA report in JSON format (Open in text editor)
Window	Report	-	Opens the Report tab.
	Status	-	Opens the Status tab.
	VFS	-	Opens the VFS tab.
	Server	-	Opens the Server tab.
Help	Help Contents	-	Opens this Help file.
	Online Knowledge Base	-	Opens the Globalscape Knowledge Base, https://kb.globalscape.com/.
	Online Support	-	Opens the Globalscape Help Center Web page, https://www.globalscape.com/support-home.
	Generate Support Data	-	Opens the Generate Support Data Wizard
	Provide Feedback	-	Opens the Globalscape Customer Support **Contact Us** page, https://www.globalscape.com/contact-us.
	Activate <product>	-	Opens the EFT Registration Wizard.
	Request Trial Extension	-	Opens the **Trial Extension Request** dialog box.
	Enter Trial Extension Response	-	Opens the **Trial Extension Response** dialog box.
	About EFT Server	-	Opens the About dialog box.

Server Tab

EFT employs an inheritance hierarchy to manage the Server, Site, and user settings, and Group permissions. The administration interface displays this hierarchy as a navigation tree in the left pane on the **Server**tab.



The tree displays each of the EFT components that you configure in the administration interface. When you click an item in the tree, the available tabs in the right pane change based on your selection. For example, when you click a Server (for example, Local Server) on the **Server** tab, the tabs appear in the right pane for configuring that Server. When you click a user on the **Server** tab, the tabs appear in the right pane for configuring that user.

You can create new items and manage items in the tree by right-clicking the tree, or clicking **Configuration** on the main menu. The illustration below shows the nodes expanded and labeled. Descriptions are below the illustration.

The **Server Group** node is the topmost level and is an organizational function for multiple groups of Servers; you can add additional Server Groups. (Do not confuse with Permission Groups, below.)

The **Server** node represents one or more physical EFT services running on the local computer or a remote system. Refer to Server Setup Wizard for more information.

The **Site** node is similar to a virtual host bound to one or more IP addresses. Multiple Sites (or hosts) are allowed within each Server. Configuration of Site-wide settings can be inherited at lower levels (in the Settings Template or per user). Each Site contains its own Settings Templates, Users, Groups, Commands, Advanced Workflows, Event Rules, Gateway node, Activity node, and Search node. Refer to Defining Connections (Sites) for more information.

The **User Settings Templates**node allows you to apply a setting configuration to an entire group of users. Similar to templates or profiles, Settings Templates are a powerful way of organizing users into groupings with predefined settings. The Settings Template specified as the default appears in the tree with bold text.

Users are individual accounts or partners assigned to a Settings Template. Each user can be configured to inherit settings from the Settings Template or have specific settings defined for that particular user. When a user account is disabled, the user icon has a red circle with an X on it . A user account without a defined email address has a blue circle with an **i**on it .

The Guest Users Settings Template is where Guest Users will appear when invited to join a Workspace and have created accounts.

The **Groups** node allows you to define user access permissions to files and folders. Groups are assigned on the Site. Users' access to folders and files are defined by their assigned Group's permissions.

The **Commands** node allows you to configure Commands that launch external executables, batch files, or scripts. Once configured, these Commands can be called from within an Event Rule.

The Advanced Workflows node allows you to design programmatic workflows visually, without prior programming experience. You can "drag-and-drop" from a list of hundreds of predefined actions to create sequenced workflows according to your business logic. Once configured, these workflows can be called as individual actions from within an Event Rule

The **Remote Agents** code allows you to configure Remote Agent templatesfor Remote Agent connections.

The **Connection Profiles** node contains the Connection Profiles that you have created.

The **Event Rules** node consists of triggering Events, optional Conditions affecting the Event Rule, and the resulting Actions that are carried out. It also contains Event Rules Folders that you have created to organize your Event Rules. For details, refer to Introduction to Event Rules.

The **Remote Agents Rules** node allows you to configure Remote Agent Event Rules specific to Remote Agents.

The **Gateway** node allows you to configure the IP address, port, and protocols used to communicate with DMZ Gateway.

The **Activity** node allows you to view transfer activity to and from the Site.

The **Search** node allows you to search the selected Sitefor a specific user, Event Rule, Command, etc.

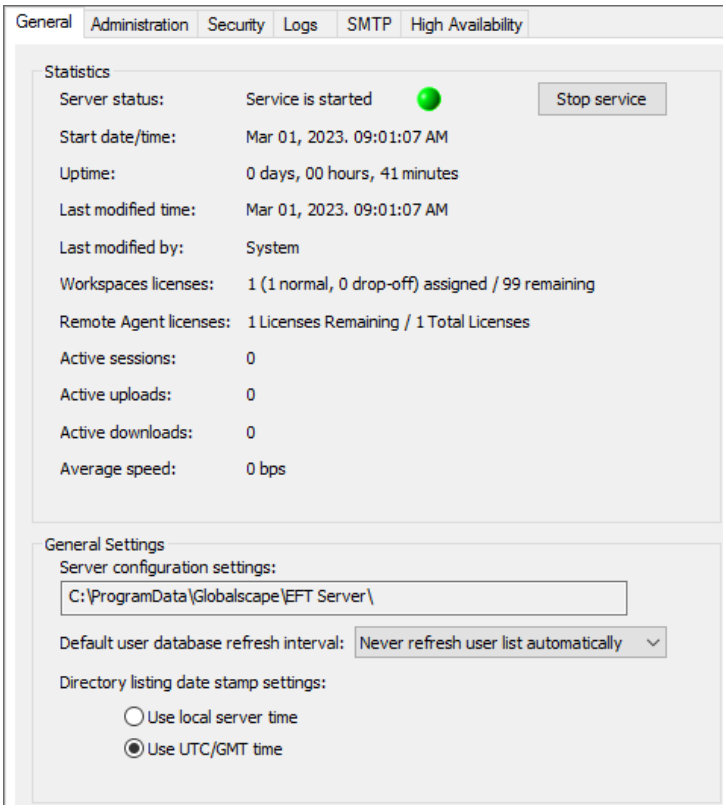
Related Topics

- Creating, Renaming, and Deleting Server Groups
- Server Setup Wizard
- Creating Sites
- Creating Settings Templates
- User Accounts and Settings Templates
- Creating Groups
- Commands
- Advanced Workflow Module (AWM)
- Remote Agents
- Connection Profiles

- Introduction to Event Rules
- Event Rules Folders
- Remote Agent Rules
- DMZ Gateway
- Viewing Transfers To and From the Site
- Inheritance
- Permission Groups

General Tab of a Server

The **General** tab of the Server node displays EFT statistics, and you can specify default messages, date stamp, and user database refresh interval. You can also stop the EFT service on this tab.



The **Server configuration settings**path is not editable in the administration interface.

Related Topics

- Stopping the EFT service
- Viewing Server Statistics
- Specifying the Default Time Stamp
- Editing the Password Reset Messages
- Editing the User Login Credentials Message
- Automatically Updating the User Authentication Database
- Workspaces Messages, Including Authentication OTP message

Administration Tab of a Server

The **Administration** tab of the Server node is used to configure remote connections to EFT, including the administration interface's IP address and port, SSL certificates, and granting or denying access by IP address, and adding, modifying, and removing Server administrator accounts.

- To view the properties of an administrator account, in the **Admin account names** area, click the account.
- To create a new administrator account, click **Add**.
- To delete an administrator account manually, click the account, and then click **Remove**.
- To remove inactive accounts automatically, refer to Removing Inactive Administrator Accounts.
- For details of the **Event Rule Change Log**, refer to Event Rules Change Log.
- To create Site administrator or other delegated administrator accounts, refer to Delegated Administration.
- To add a **Programmatic API Policy**, refer to Enabling REST API for Remote Admin.
- To enable an administrator account manually, click the account, and then click on **Enable**.
- To disable an administrator account manually, click the account, and then click on **Disable**.

For EFT-managed administrator accounts only ("EFT only"):

- To change the password of an administrator account, click the account, then click **Change Password**.
- To change the account security settings, click **Account Policy** and refer to Lockout an administrator Account.
- To change the password settings, click **Password Policy** and refer to Enforcing Complex Passwords for Administrator Accounts, Enforcing Password Reset for administrator Accounts, and Expiring Administrator Passwords.
- To change the administrator's account details manually, click the account, and then click on **Account Details**.

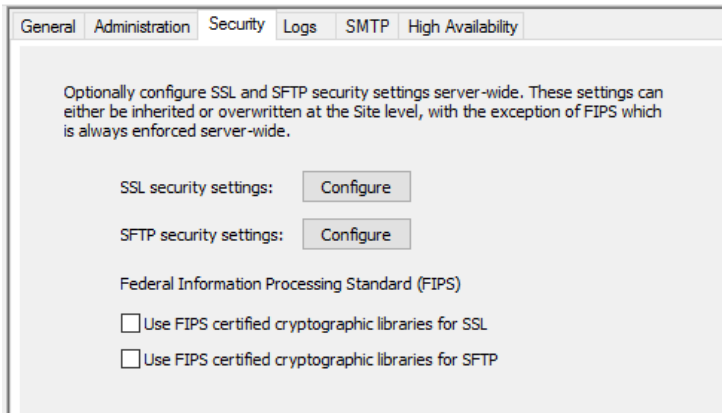
Related Topics

- Server Administration Connectivity
- Configuring Server Administrators
- Administrator Account Permissions

- Optional Permissions for Administrator
- Remote Administration
- Delegated Administration

Security Tab of the Server

The **Security** tab of the Server node is used to specify SSL versions and allowed ciphers for EFT's Sites, to enable FTPS protocol specific settings, and to enable FIPS for SSL and/or SSH.

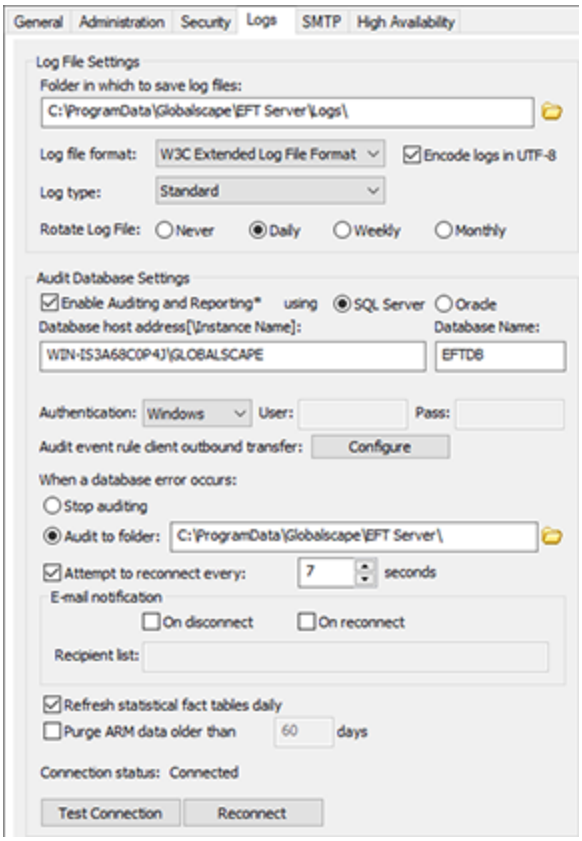


Related Topics

- Enabling SSL on the Server
- Enabling SSL on the Site
- Configuring SFTP for a Site
- Enabling SFTP on the Server
- Creating Certificates
- SSL Certificates
- Explicit Versus Implicit SSL
- Certificate Chaining
- Connection Problems
- FIPS-Certified Libraries

Logs Tab of a Server

The **Logs** tab of the Server node is used to configure the type and location for the Server logs and Auditing and Reporting settings.

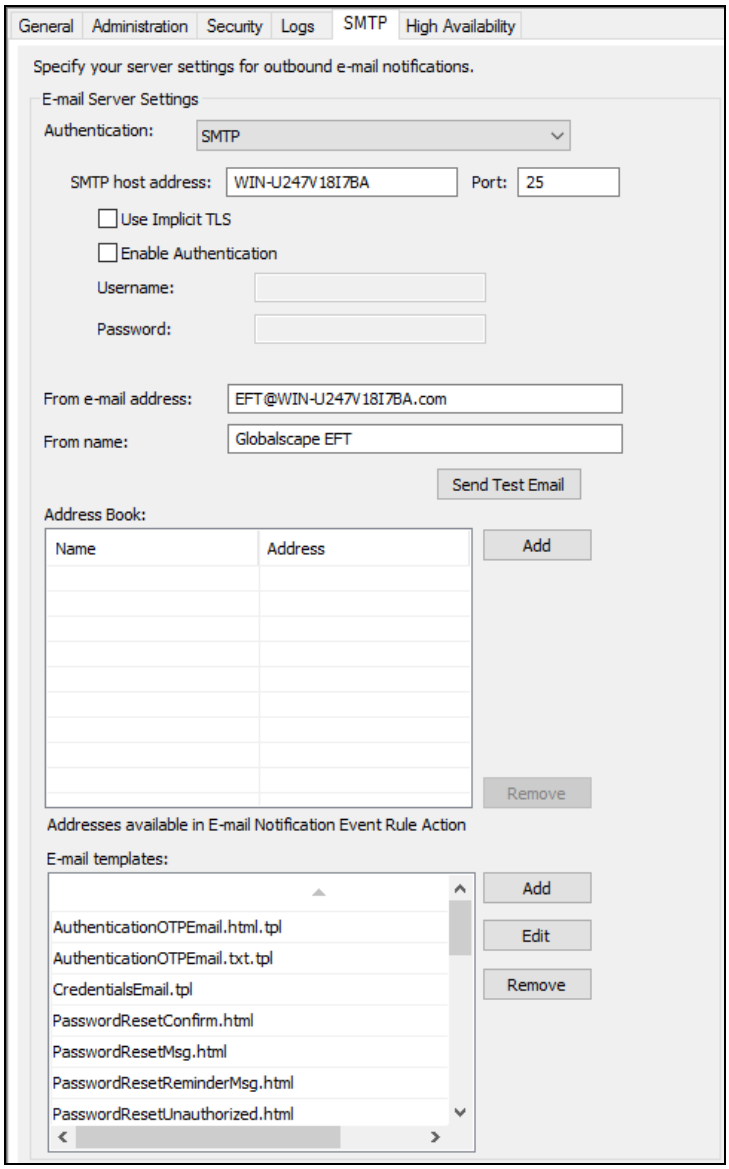


Related Topics

- Log Settings
- Audit Database Settings
- EFT Logging and Visibility
- Auditing Database Errors and Logging

SMTP Tab of a Server

The **SMTP** tab of the Server node is used to specify the mail server settings that EFT uses to send email notifications, and the email templates to use with notifications. When you create EFT in the **Server Setup Wizard**, the mail server settings on this tab are automatically populated.



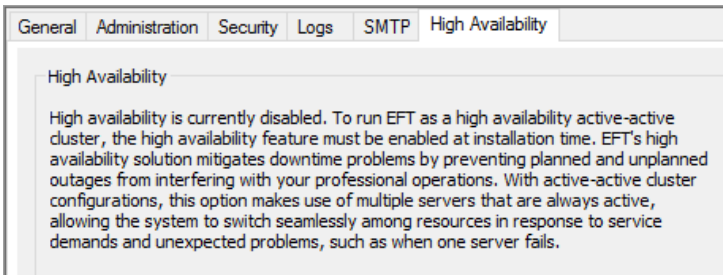
- Click the **Authentication** drop-down box and select **SMTP**, **Gmail OAuth**, or **Office 365 OAuth** for outgoing mail, then refer to Email Server Settings for details of configuring one of those options for outgoing mail.

High Availability Tab of a Server

The **High Availability** tab of the Server is a read-only tab that displays the configuration for high availability (active-active) clustering of EFT. The tab contains the multicast address, port, and listening queues, as well as the default paths for load balancing.

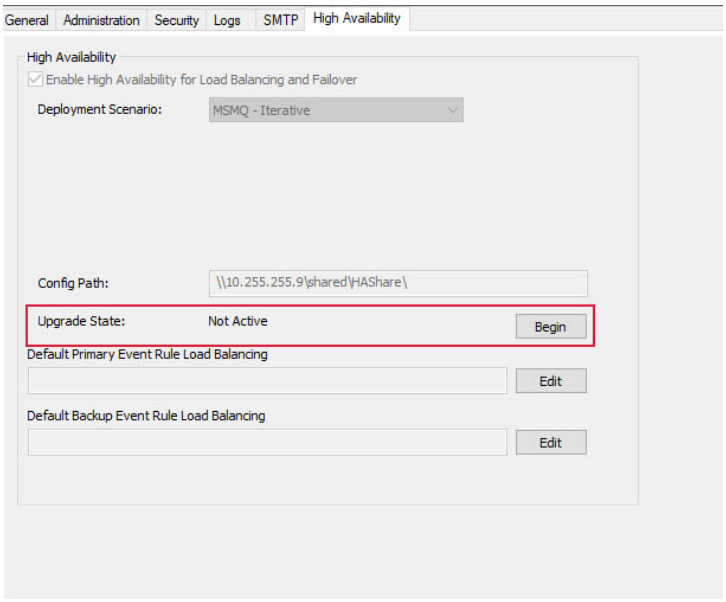
Stand-Alone Server:

If HA is disabled, a message appears explaining that HA is disabled.



HA Server:

If EFT is installed as an active-active or active-passive cluster, the fields below will be displayed.



Deployment Scenario—Displays either MSMQ or Unicast

Multicast Address—The address for the group of nodes in the cluster.

Multicast Port—The port used by the multicast address.

Coherence Queue—Repository for the message queuing (MSMQ) cache that broadcasts messages across the HA cluster to keep all nodes in sync.

Event Queue—Repository where events are held prior to processing.

Config Path—Path at which the cluster's shared configuration is stored.

Upgrade State—If you are upgrading the cluster, click **Begin** to put EFT in read-only mode to begin the upgrade process. The button will display **End** when the upgrade has completed. During upgrade, Upgrade State will display “Active; Outdated; x.x.x.x”, where x.x.x.x is the current EFT version.

Default Primary Event Rule Load Balancing—Here you can click **Edit** to specify the primary node(s) to run load balanced Event Rules.

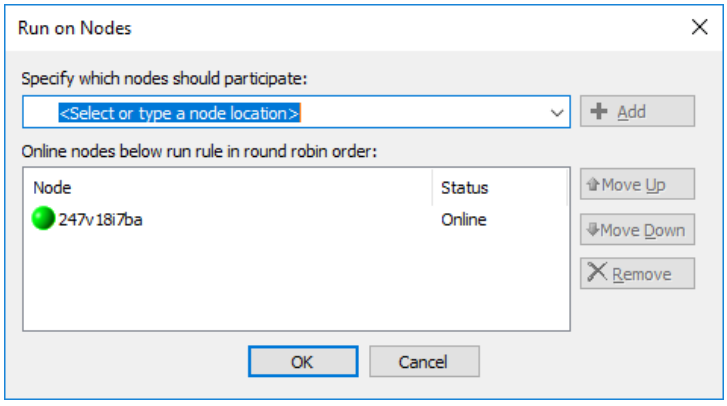
Default Backup Event Rule Load Balancing—Here you can click **Edit** to specify the backup node(s) to run load balanced Event Rules.

- Event Rules will use these default node lists. If the default node list is empty, the Event Rule will execute on ALL nodes of the cluster unless you explicitly specify which node is to run the Event Rule when you define the Event Rule.

To define the default Event Rule load balancing nodes

1. In the administration interface, connect to EFT and click the **Server** tab.
2. Click the **High Availability**tab.

   Next to the **Default Primary Event Rule Load Balancing** and **Default Backup Event Rule Load Balancing**, click **Edit**. The **Run on Nodes** dialog box appears.



3. Click the down arrow to select a node, click **Add**, then click **OK**.

Related Topics

- High Availability Overview
- HA FAQ
- Server Drain, Maintenance, and Auto-Restart
- Unicast
- High Availability Message Queuing
- Active-Active HA Cluster—Installing or Upgrading the Server
- Upgrade an HA Cluster with Zero Downtime
- HA-Related Knowledgebase Articles
- Event Rule Load Balancing

Automate Service Account

The Automate Desktop service (also known as the Task Service, AMTS.exe) enables tasks created using Automate Desktop to trigger automatically on the computer. If this service is stopped, Automate Desktop tasks will not be run at their scheduled times.

To continue to run EFT event rules when the Windows session is logged out or locked, or the EFT server service account is logged out, ensure that the *Automate Service Account* (described below) is enabled on the **Server > Administration** tab in the EFT administration interface.

> **NOTE:** EFT administrators should not modify the Automate Desktop 2024 service in the Microsoft Manage Console **Services** dialog ("Log on As") as this will break functionality. Refer to the Knowledgebase article #11645 Modifying the Automate Desktop 2024 service account breaks functionality for more details.

Before creating or using Advanced Workflows in EFT, you should wait a while after any of the following actions have occurred:

- When an EFT site is getting started (every time a site is started), it sets the Automate license and triggers an Automate service restart. Therefore, after a site is started, don't immediately open any Advanced Workflow tasks or Event Rules containing Advanced Workflows. It simply won't work, because it might be that the Automate service has not yet started, because this may take some time.
- Any changes to an EFT license, extending or deregistering the trial, or registering or deregistering the Advanced Workflows module will set the Automate license expiration dates accordingly and trigger Automate Service restart. Meaning that after any of those actions, you may have to wait until the Automate service gets started.
- Automate service is started or restarted in each of the cases described above and on EFT site start.
- Automate service is started or restarted when an Event rule is triggered, but for some reason Automate service shows it has stopped. Then EFT restarts it and then re-triggers the Event rule.

The Automate service enables tasks created using the Task Builder to trigger automatically on the computer. If this service is stopped, tasks will not be run at their scheduled times. **The Task Builder requires a valid Windows user account to be**

enabled on the computer on which it is running to execute Advanced Workflows in event rules.

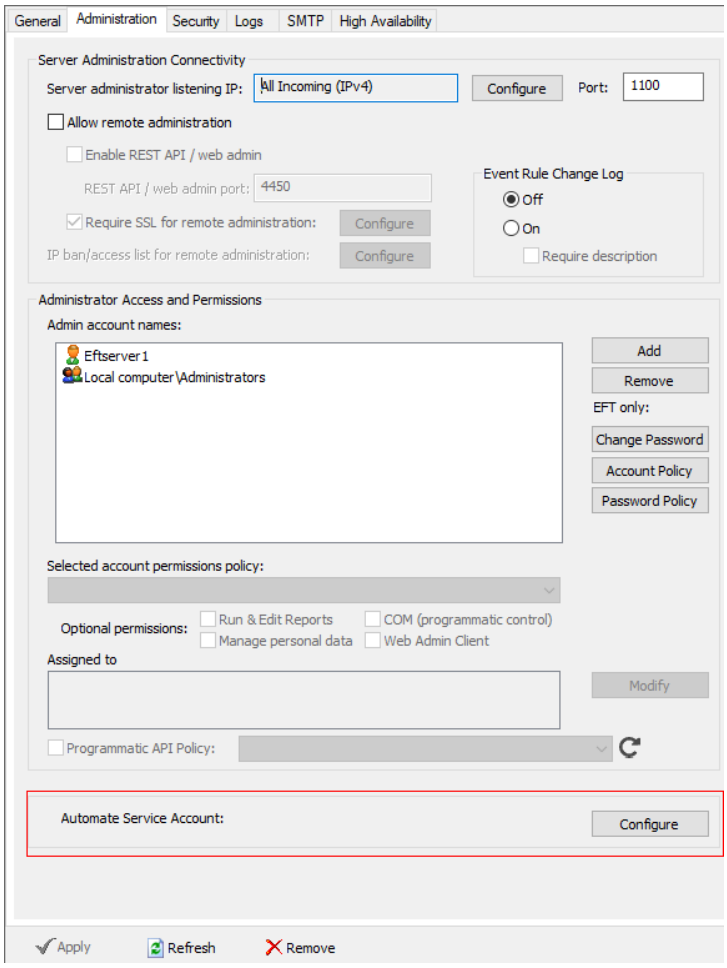
When the EFT administrator account or EFT service account has logged off of a Windows session, an *Automate service account* is needed to execute Advanced Workflows via event rules. EFT provides a way for the administrator to enter credentials for a Windows user account and persist them as part of EFT's configuration. The Automate Service account is enabled in the EFT administration interface on the **Server > Administration tab**.

For example, the AWM **Dialog** action requires user input, which is not desired since the EFT administration interface is not continuously monitored and a user prompt could delay the completion of event rules. You should enable the Automate Service Account in EFT to prevent the Dialog pop-up from occurring. Tasks will run in the background without popups.

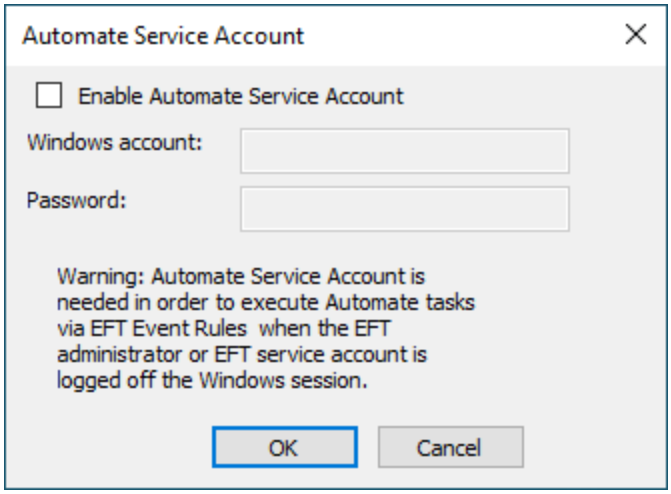
> **NOTE:** The Automate Service Account (in EFT) is a local system account and is not synchronized between clusters.

To enable the Automate Service Account

1. At the bottom of the **Server > Administration** tab, next to **Automate Service Account**, click **Configure**.



The **Automate Service Account** dialog box appears.



2. Select the **Enable Automate Service Account** check box.
3. Provide the **Windows account** name and **Password** to be used for the Automate service account.

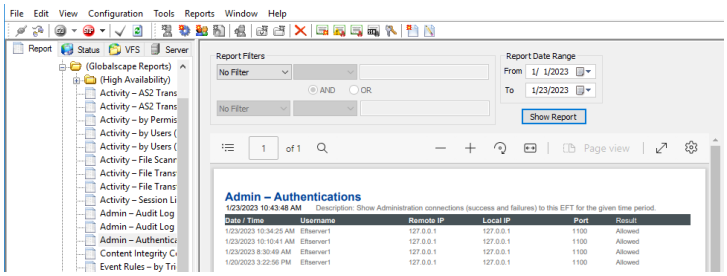
> **NOTE:** The Automate Service Account is a local system account and is not synchronized between clusters.

4. Click **OK** to close the dialog box and then click **Apply** to save the changes.

   Tasks will run in the background without popups.

Report Tab of a Server

The **Report** tab is the interface to the Auditing and Reporting module (ARM). The **Report** tree in the left pane lists the predefined Globalscape Reports and your custom reports. When you select a report in the left pane, the right pane updates for you to specify filters and a date range, and to show the report, which you can then save as an HTML, VP, PDF, or TXT file.

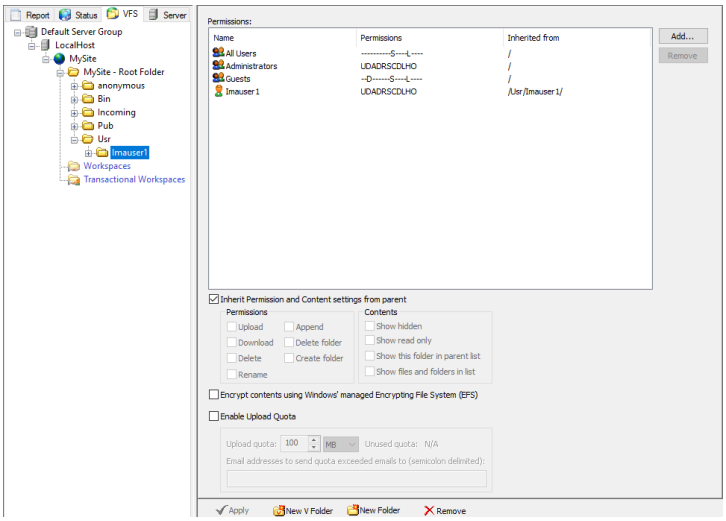


Related Topics

- Descriptions of Preconfigured Reports
- Generating a Report
- Filtering a Report
- Custom Reports
- Managing Reports

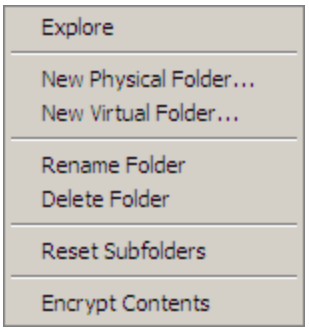
VFS Tab of a Server

The **VFS** tab is the interface for the Virtual File System (VFS), used to grant access to files and folders on your system. Click a folder in the left pane, then the permissions for that folder appear in the right pane.



- The left pane displays the physical folders for the Site and any virtual folders that you have defined.
- In the right pane, you add and remove users and permissions groups and set their permissions. (The default groups are displayed automatically.)
- The bottom toolbar provides options to create a new virtual or physical folder, and to remove a selected folder.

Right-click a folder in the left pane to open the sub menu that provides Virtual Folder options:



- **Explore**- Opens Windows File Explorer to view the contents of the selected folder.

- **New Physical Folder** - Creates a new physical folder
- **New Virtual Folder** - Creates a new virtual folder
- **Rename Folder** - Allows you to edit the selected folder name
- **Delete Folder** - Deletes the selected folder
- **Reset Subfolders** - Resets permissions on the subfolders of the selected folder
- **Encrypt Contents** - Encrypts the contents of the selected folder (and allows you to specify whether to also encrypt subfolders)

Related Topics

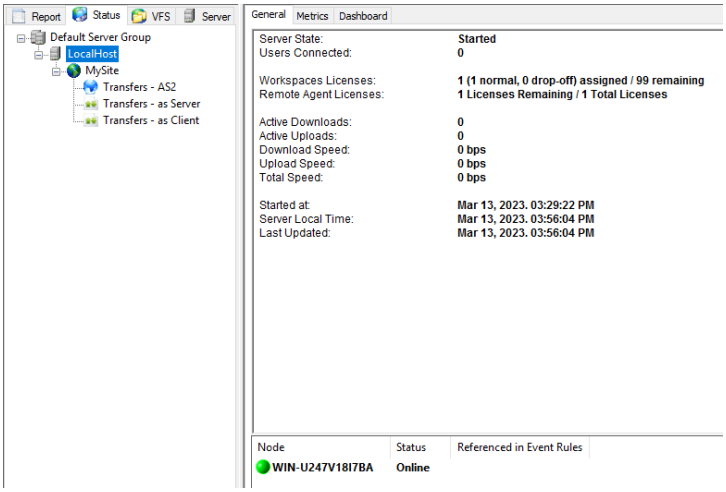
- Introduction to the Virtual File System (VFS)
- Modifying VFS Permission
- Permission Groups
- Setting VFS Folder Permissions
- Resetting VFS Folder Permissions
- Streaming Repository Encryption
- WTC & Workspaces - Sharing Files & Folders

Status Tab of a Server

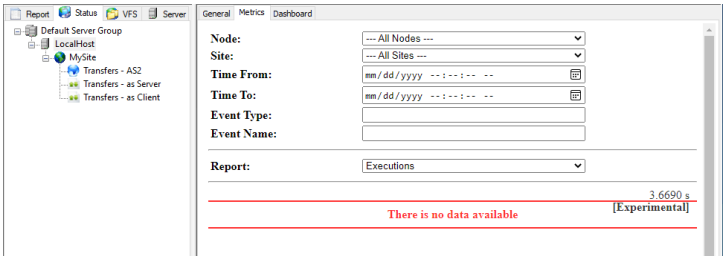
The **Status** tab contains nodes for each Server Group, Server, Site, AS2 transactions, Transfers as Server, Transfers as Client, and each logged-in user.

If you expand the **Site** node, you can view the connection status for the Site, users, and for AS2 transactions. You can also view transfers to and from an EFT Site. Refer to Viewing Transfers To and From the Site for details.

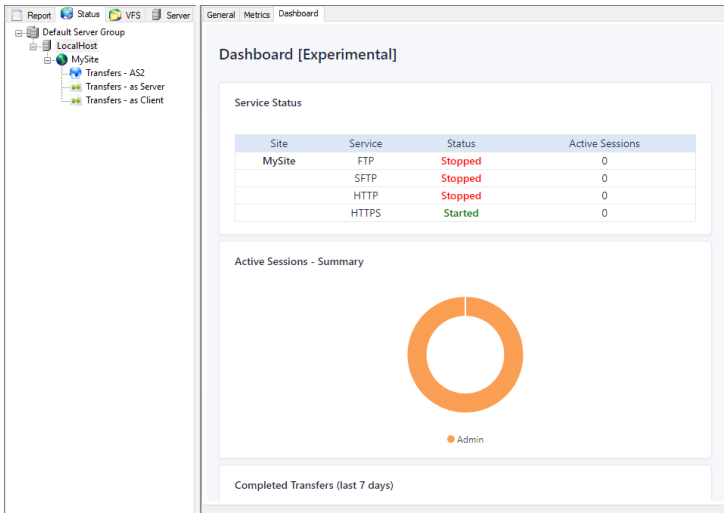
- The **General**tab on the **Server > Status** tab is used to view the status of the selected server, and the status of the node.



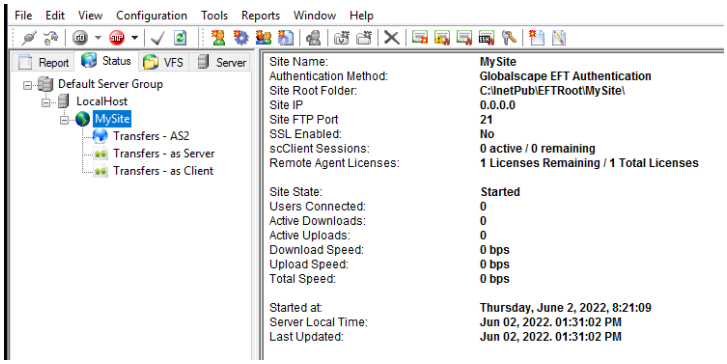
- The **Metrics** tab of the **Server > Status** tab displays metrics from the ARM database. (You must have historical data.)



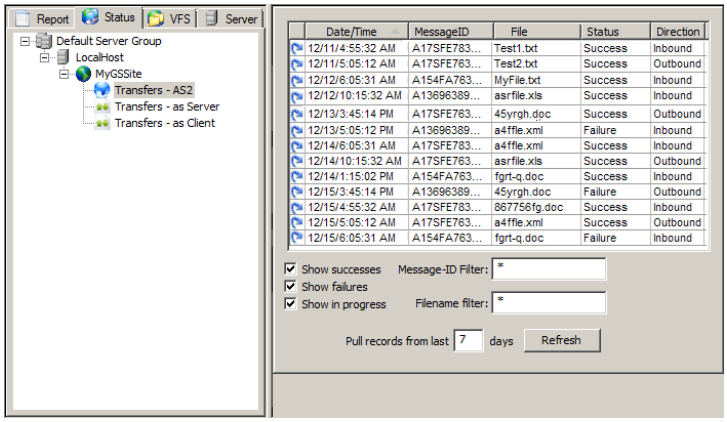
- The **Dashboard** node of the **Server > Status** tab is a visual display of the service status, active status, and completed transfers.



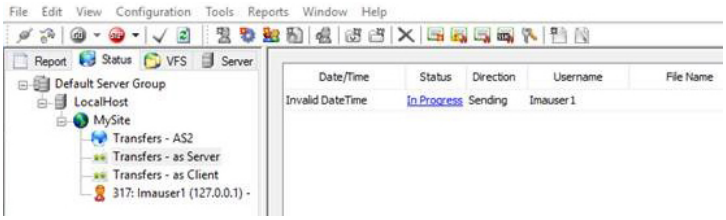
- The **Site** node on the **Status** tab of the administration interface is used to view the status of the Site and logged-in users, including transfers, when EFT was started, number of users connected, and so on. You can also forcibly disconnect FTP/SFTP users from the Site on this tab.

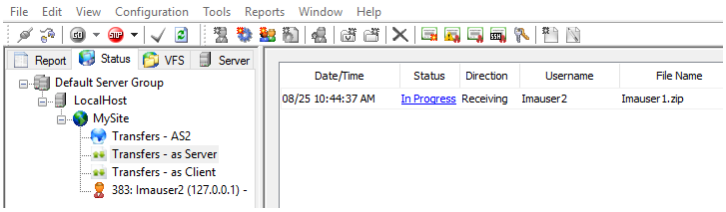


- The **Transfers - AS2**node is used to view the status of attempted AS2 transactions. For details of viewing AS2 transaction history, refer to AS2 Transaction Auditing and Monitoring.



- The **Transfers - as Server** and **Transfers - as Client** nodes are used to view transfers on the Site. (Real-time client transfers require the Auditing and Reporting module).
    - As of EFT 8.3.0 the Transfers – as Client now provides a column to display Event Rule Name that are triggered.



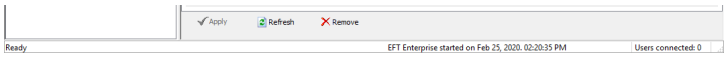


Related Topics

- Server Statistics
- Monitoring User Connections
- Forcibly Logging a User Off of EFT
- AS2 Transaction Auditing and Monitoring
- Resubmitting AS2 Transmissions
- Viewing Transfers To and From the Site

Status Bar

The **Status** bar is displayed across the bottom of the administration interface to indicate whether you are connected to EFT, the date and time EFT started, and how many clients (users) are connected to EFT via FTP.



"Ready" appears in the lower left area of the **Status**bar when the application is idle (that is, no Windows messages are being processed at the time). If the interface is busy processing information, the "Ready" area of the **Status**bar can be blank.

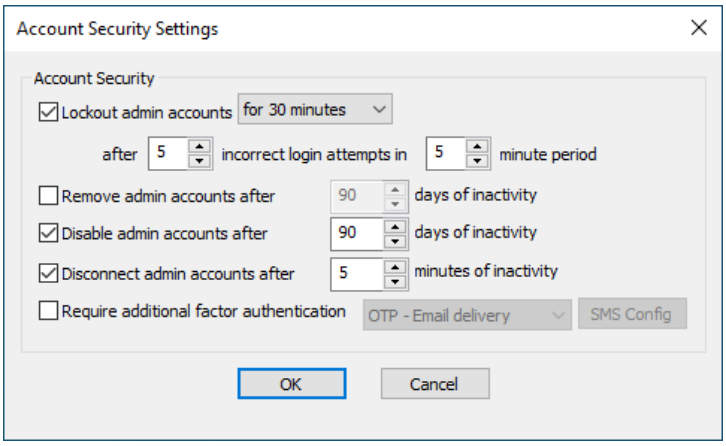
Administration Interface Session Timeout

EFT incorporates an internal idles timeout of 5 minutes for administrator connections via the administration interface connections with high security-enabled Sites. On Sites defined using "strict security settings," if no activity (such as OnMouseClick) occurs after 5 minutes of inactivity, a warning message and countdown timer appear. The timer resets if you click **Continue**; if no activity occurs, the timer expires, and the administration interface disconnects from EFT. Any non-committed changes are discarded.

This is different from the Administration Interface Session Timeout value set for the user and Settings Template.

To change the timeout

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure, and then click the **Administration** tab.
3. Click an EFT-managed administrator account, and then click **Account Policy**. The **Account Security Settings**dialog box appears.



4. Select the **Disconnect administrator accounts after** check box, then specify the minutes of inactivity you need. (In versions prior to 8.0.5.8, the check box is cleared by default for non-high security enabled Sites.) Changing the timeout to more than 15 minutes violates PCI DSS, so you will need to document the reason/compensating control if you have a high-security-enabled Site.
5. Select **Require additional factor authentication** check box to configure multifactor authentication for administrator accounts.
6. Click **OK** to save the changes.

Related Topics

- Disconnecting Users on Timeout
- Logging Out of EFT
- Closing the Administration Interface

Closing the Administration Interface

The administration interface will automatically close your connection after 15 minutes of inactivity, but the EFT service continues to run in the background. A warning message and countdown timer appear 5 minutes before the connection times out.

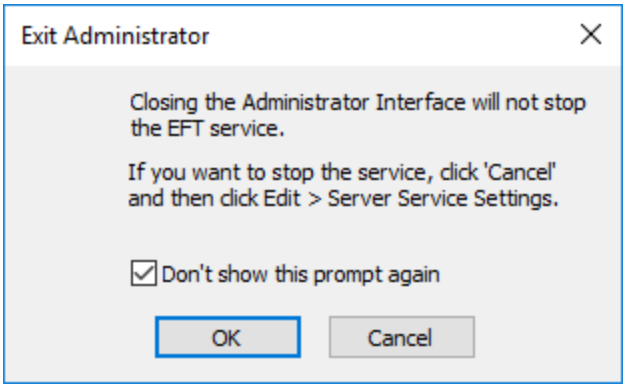
When you manually close the administration interface, you can configure an **Exit Administrator** confirmation prompt. You can turn this prompt off for future exits from within the prompt or in the **Server Global Settings**dialog box.

> **NOTE:** If you exit by clicking the server disconnect icon in the upper left corner , there will not be a prompt; it will just close.

To close the administration interface

1. Do one of the following:
   - In the upper right corner of the administration interface, click the **X**.
   - On the main menu, click **File >Exit administrator**.

   The **Exit administrator** dialog box appears.



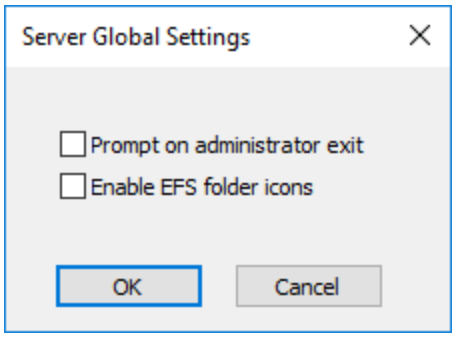
2. If you do not want the **Exit administrator** dialog box to appear when you close the interface, select the **Don't show this prompt again** check box; otherwise, leave it selected.
3. Click **OK**. The administration interface closes.
4. To turn the prompt back on, refer to the procedure below.

Configuring Exit Prompts

In the **Server Global Settings** dialog box, you can specify whether you are prompted when you close the administration interface.

To configure login or exit prompts

1. On the main menu, click **Edit >Global Settings**. The **Server Global Settings** dialog box appears.
2. The **Prompt on administrator exit** check box is cleared by default. If you want a message to appear when you close the interface explaining that the EFT service does not stop after the administration interface is closed, select the **Prompt on administrator exit** check box.



3. Click **OK**.

Web Administration Console (WAC)

The EFT "Web Admin" console allows EFT administrators to manage EFT remotely over the internet. No need to install a separate desktop tool.

- Configure EFT to Use Web Admin
- Logging in to Web Admin
- Overview Page
- User Management Page
- View Site and Node Health
- View Connected Users
- View Active Automation Rules
- View Transfers

Configure EFT to Use Web Admin

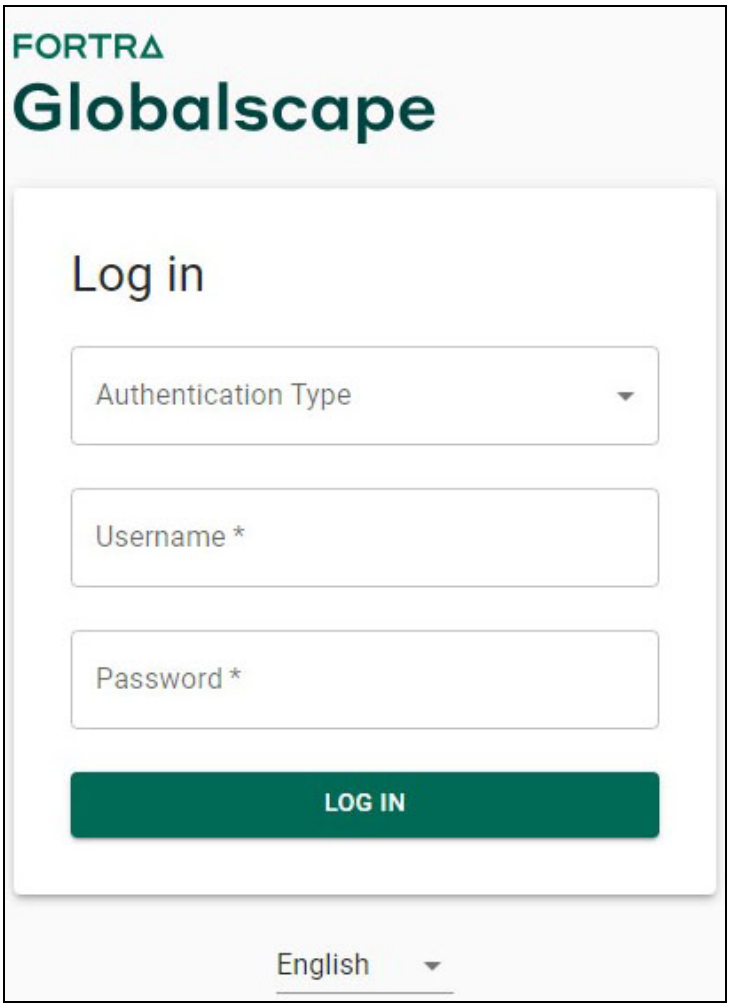
The Web Admin console is based on the REST API, so you must have REST API configured in the EFT administration interface, on the Server > Administration tab.

To configure EFT to use the Web Admin

1. Log in to the EFT administration interface, then click the **Server > Administration** tab.
2. Select the **Allow remote administration** check box.
3. Select the **Enable REST API / web admin** check box.
4. In **REST API/web admin port**, specify the port number if it is different from the default (4450).
5. Select the **Require SSL for remote administration** check box, and create or specify the SSL certificate.
6. In **Administrator Access and Permissions**, select the admin account(s) that need to administer Web Admin, then select the **Web Admin Client** check box, and the **Programmatic API Policy**, and then select **server_full_access**.
7. Click **Apply** to save these settings.

Logging In to the Web Admin Console

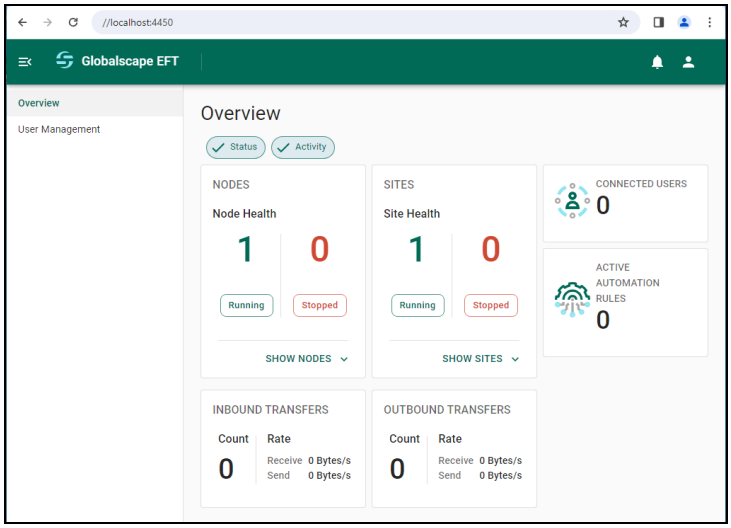
Web Admin is a browser app. You do not have to log in to EFT to access Web Admin. The EFT administrator must ensure that the EFT server service is running and should have Configured EFT to Use Web Admin in the EFT administration interface, on the **Server > Administration** tab.



To log in to Web Admin

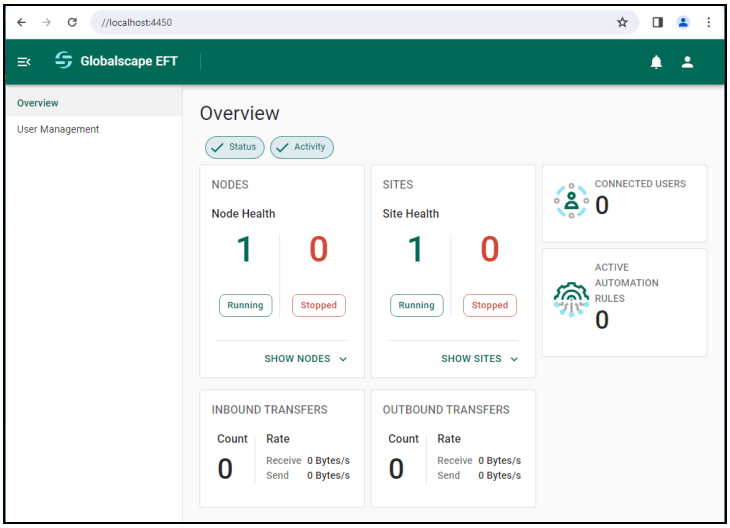
1. Open a browser and go to the server: port provided to you by your EFT admin. (For example, on the EFT computer, https://localhost: 4450.) The **Log In** dialog box appears.
2. Specify your **Authentication type:** EFT Authentication or Active Directory.
3. Provide the username and password of an EFT server administrator account.

4. Click **Log In**.
5. The Web Admin **Home** page appears.



Overview

The Web Admin Overview page displays information about EFT and its Sites, Nodes, transfers, automation rules, and users.

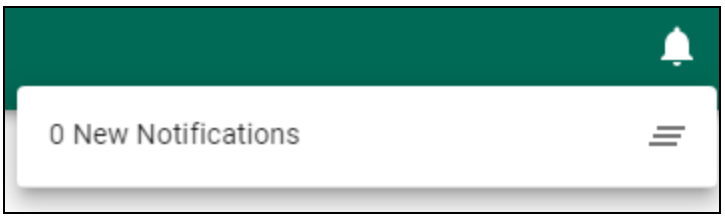


The **Overview** page displays information about the server and sites that you have configured in EFT, depending on the administrator account type.

- Server level admin - can see everything
- Site level admin - nodes widget is gone; you see counts only for resources you have permission to
- Any other level admin - home page is not available; immediately redirected to user management; option on left menu for Overview disappears
- The widgets refresh every 30 seconds. (Hard-coded, cannot be changed.)
- The icon in the upper left corner of the title bar allows you to close or open the left menu.

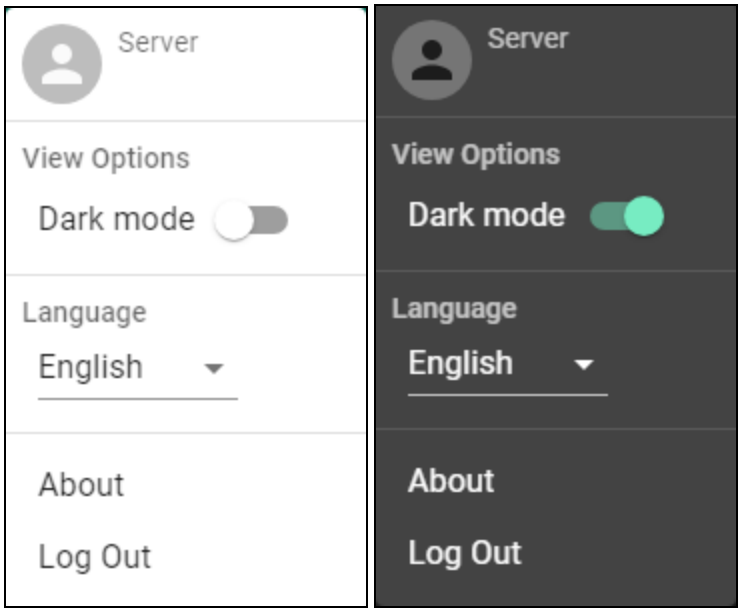
The **Sites** menu allows you to specify a Site to monitor when you have multiple Sites defined in EFT.

The bell icon opens the notifications panel:



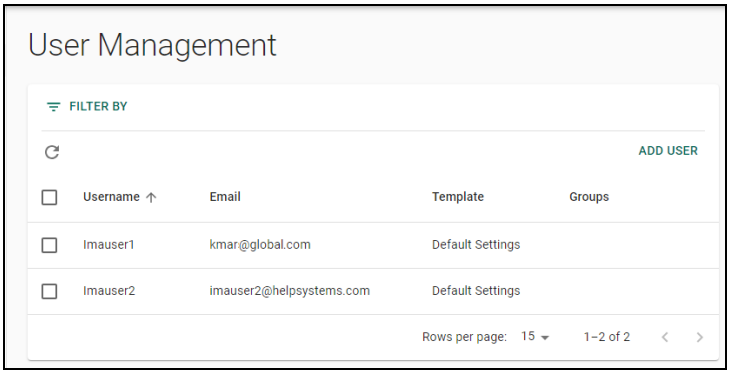
The user icon opens a drop-down menu to view:

- Username of the logged in user (you)
- **View Options** - Dark or light theme
- **Language** - Languages supported as of v8.2 include English, Spanish (Castilian), German, French (Standard). The WAC defaults to English when you first log in. Then it will always pull from local storage. For example, if you set it to German, it will still be in German the next time you log in (on the same browser).
- **About** - Version number of Web Admin and copyright notice
- **Log Out**



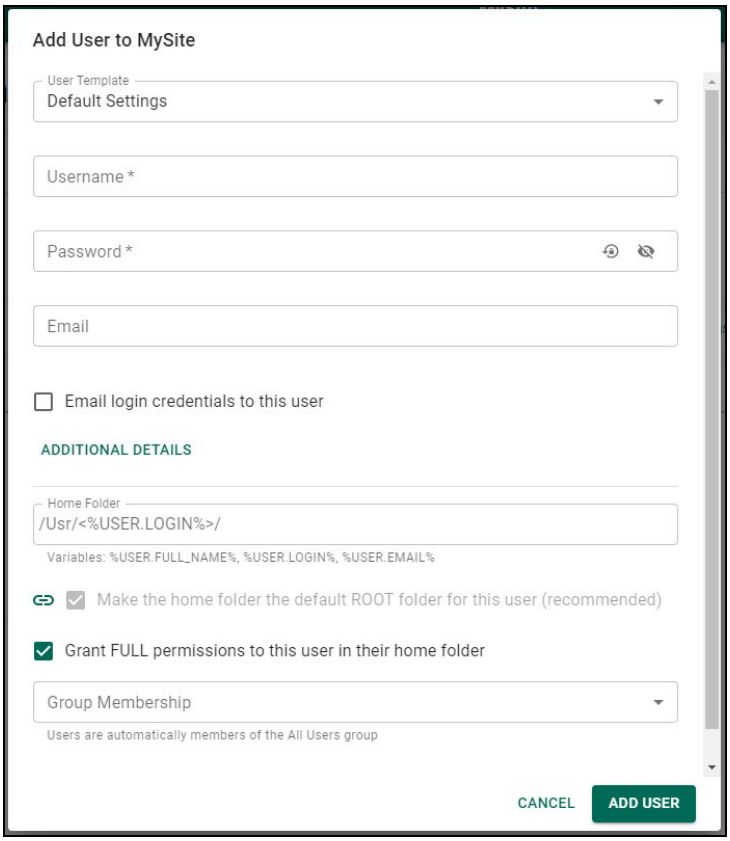
User Management

The User Management page displays information about defined user accounts, and allows you to add, edit, and delete users.



To Create a User

1. Click **Add User**. The **Add User to** [MySite] dialog box appears. ("MySite" is replaced with name of your site).

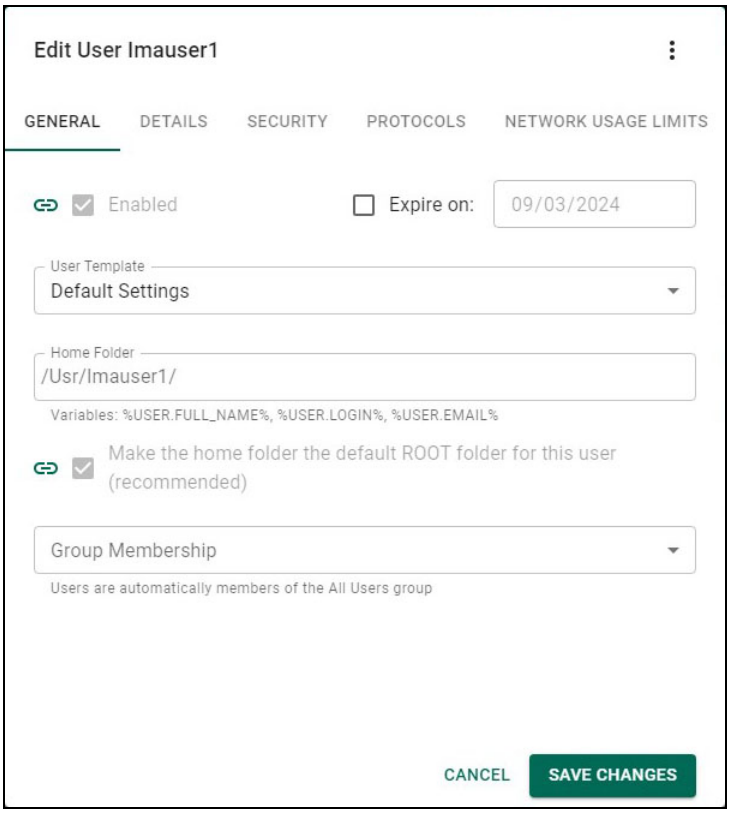


2. Specify the **User Template** to which you will assign this new user. Templates are defined in EFT. (Default Settings and Guest Users are created at installation of EFT).
3. Provide a **Username**, **Password**, and **Email** address for the account.
4. Select the **Email login credentials to this user** check box to send the user their credentials.
5. **Grant FULL permission to this user in their home folder** is selected by default. (If you do not grant users full permissions to their home folders, they will inherit their Group's permissions).
    - New users are automatically members of the **All Users** group. In the **Group Membership** drop-down list, you can (optionally) add them to the **Administrators** group and /or the **Guests** group. (This setting is separate from the **Guests** User Settings Template).
6. The new user will appear on the **User Management** page.

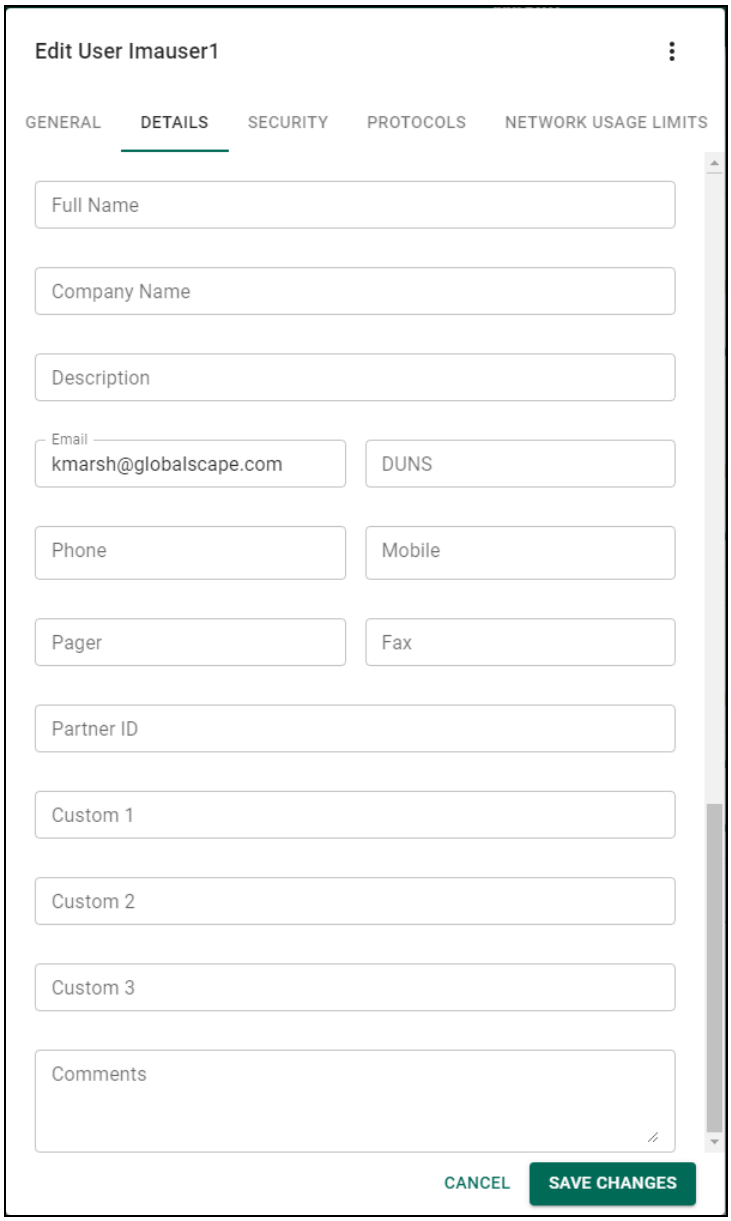
> **NOTE:** The following characters are NOT supported in the username: `{ } | [ ] \ < > / : ; " ' * + =`Username length is limited to 149 characters. The email address box cannot contain more than 255 characters.

To Edit a User

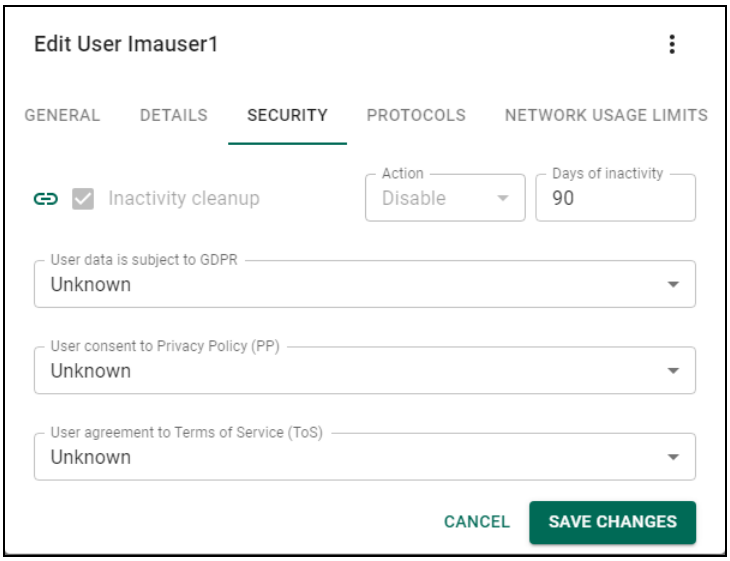
1. *Select the check box on the user's row, then click **Edit** or click the **Edit** icon* *. The **Edit User** <username> dialog box appears.*



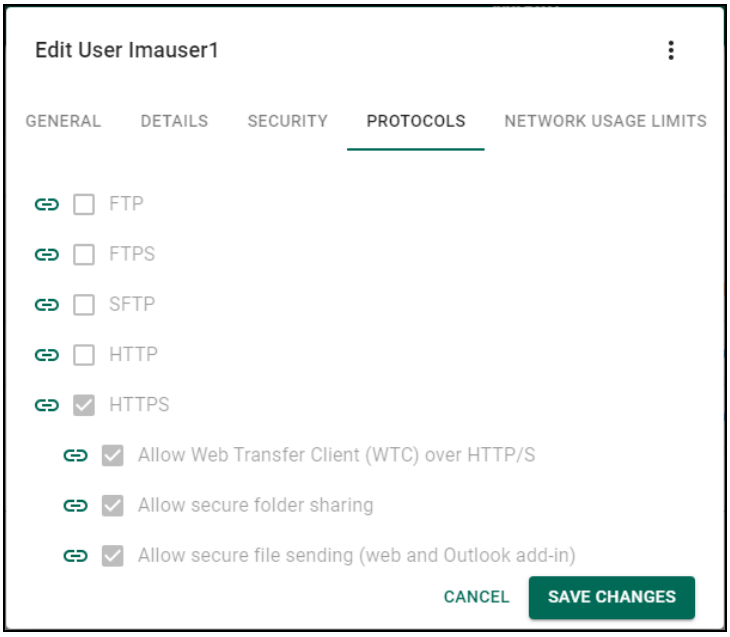
2. On the **General** tab, edit the properties of this user, as needed, then click Edit User to apply.
3. Click the **Details** tab.
4. On the **Details** tab, you can add or edit information about the user, such as full name, and phone number. (Similar to **User Account Details** in the EFT administration interface).



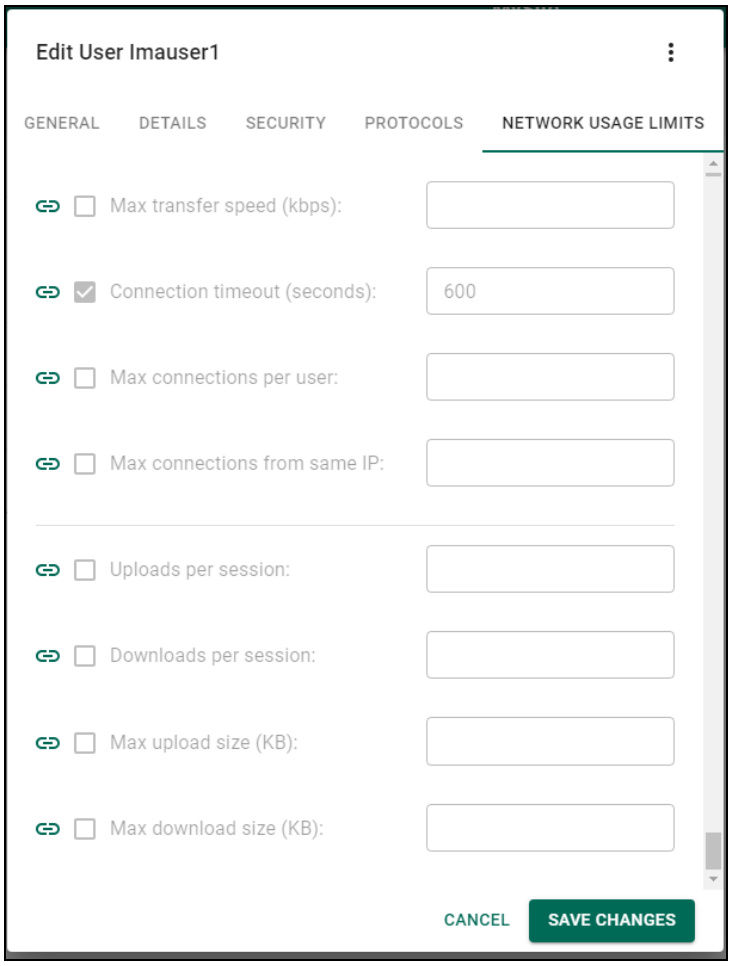
5. On the **Security** tab, you can specify if the user is subject to GDPR rules, and whether they consented to the Privacy Policy or Terms of Service. The **Inactivity cleanup** option allows you to **Disable** or **Remove** a user account if they have had a certain number of days of inactivity.



6. The **Protocols** tab displays which protocols and HTTPS features are enabled for the user. The link to the left of each protocol indicates whether it was inherited from the Settings Template or Site.



7. The **Network Usage Limits** tab enables you to configure specific limits for this user, or keep the setting from EFT from their User Settings Template. The crossed-out link icon represents whether the limit is inherited or not. If you want to keep the setting in EFT, do not select the icon (The slash will go away and the link will change color).

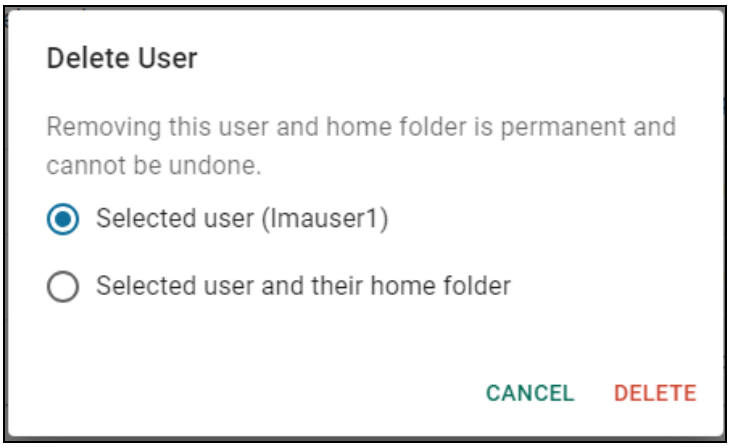


8. After making changes to any tab, click **Edit User** to save the settings.

To Delete a User

> **NOTE:** Specifying to remove the user and their home folder is permanent; the user is also removed from EFT, not just the Web Admin interface.

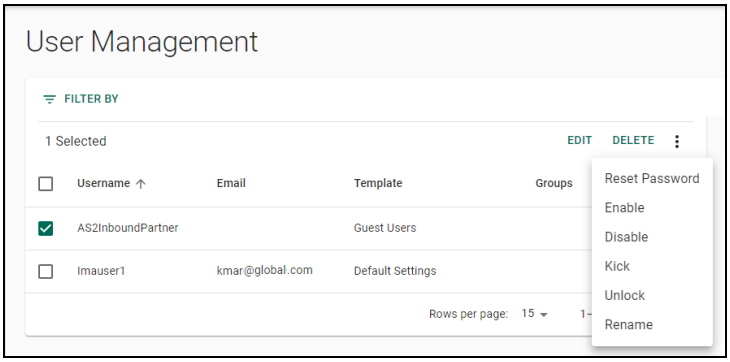
1. Select the check box on the user's row, then click **Delete**. The **Delete User** dialog box appears.



2. Specify whether to delete only the selected user, or the user and their home folder.
3. Click **Delete** to apply.

Other User Management Options

Select a username check box, then click the three vertical dots to view other options.



Using this drop-down menu, you can reset the user account password, enable the account, disable the account, kick the user off of EFT, unlock the account, or rename the account.

Reset Password

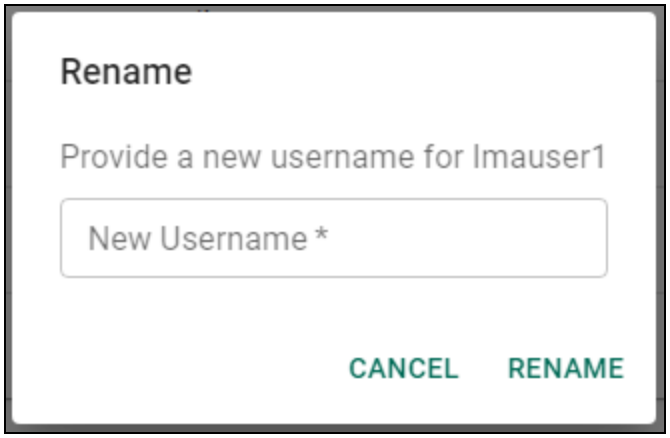
To reset a user password:

1. Select the user for whom you want to reset the password.
2. Click the three vertical dots, then click Reset Password.

> **NOTE:** If there is no email associated with the account, the password cannot be reset. Always add the user password to the account when you create the account. In the case of a missing email address, you will have to log in to the EFT Administration interface to add the email address and change the password.

Rename

In the **Rename** dialog box, provide a new username, then click RENAME.



Enable

If an account has become disabled because of expired Workspaces links (for example), click **Enable**.

Disable

If an account needs to be disabled (such as an inactive account), you can disable it here.

Kick

Use **Kick** if you want to manually disconnect a user from EFT.

Unlock

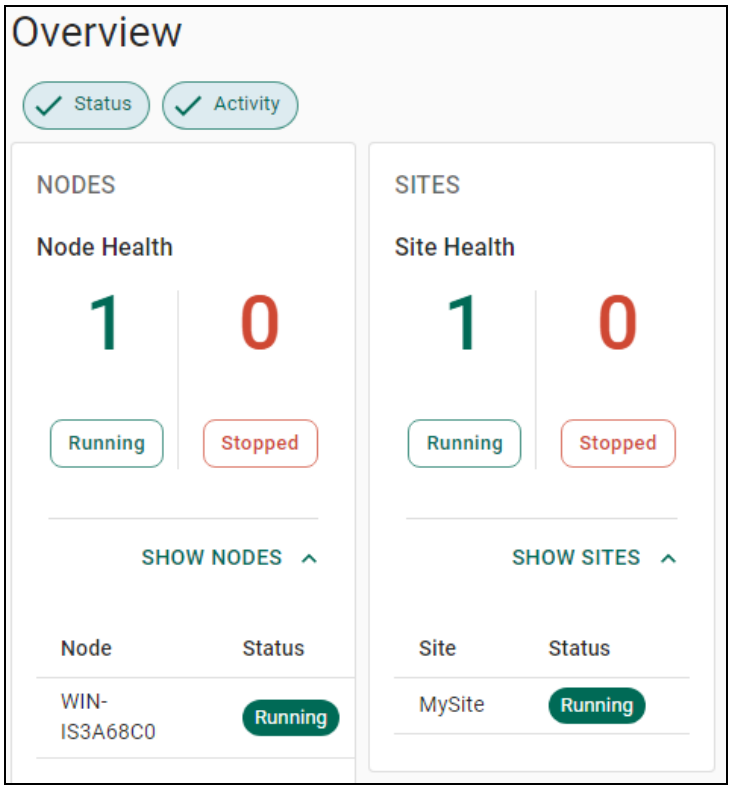
A user account can be locked out from too many invalid password attempts. Click **Unlock** to unlock their account.

> **NOTE:** You can change the lockout parameters on the **Settings Template > Security** tab **Invalid login options**. The default is to lockout the account for 30 minutes after 5 invalid attempts in 5 minutes. (Maybe reset the account password also).

View Site and Node Health

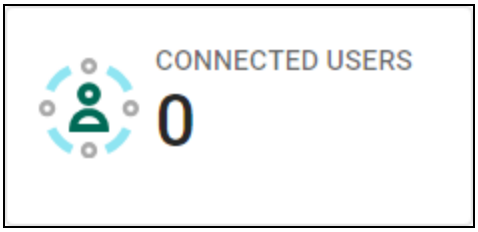
You can view the Site and Node health on the **Overview** page.

To view Site or Node health click **SHOW NODES** or **SHOW SITES**. The menu will expand to display the Nodes/Sites on the server and if they are running or stopped.



View Connected Users

The **Overview** page displays the number of connected users.

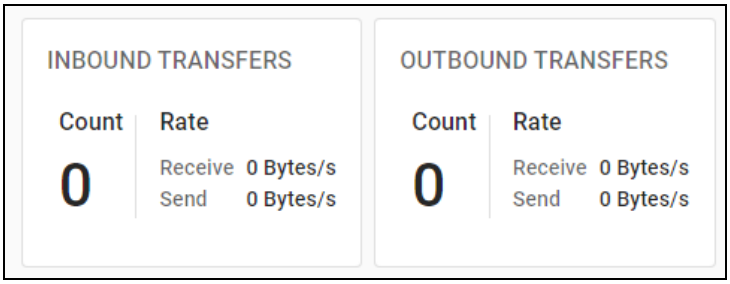


View Active Automation Rules

The **Overview** page displays the number of active automation rules.

View Transfers

The **Overview** page displays the number of and transfer speed of inbound and outbound transfers received and sent.



Administrator Account Configuration

This section describes procedures for creating and managing EFT server administrator accounts.

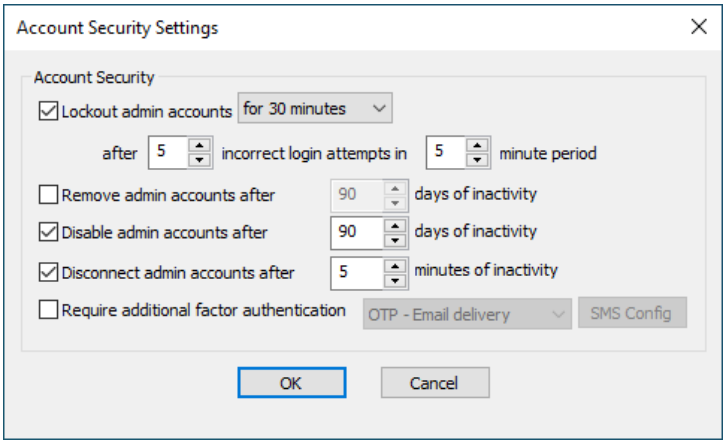
- Account Security Settings Dialog Box
- Active-Directory Based Administration
- Creating EFT Administrators
- Administrator Account Permissions
- Delegated Administration
- Optional Permissions for Administrator
- Changing an Administrator Password
- Enforcing Complex Passwords for Administrator Accounts
- Enabling Password History for Administrators
- Enforcing Password Reset for Administrator Accounts
- Expiring Administrator Passwords
- Resetting the EFT Administrator Password
- Local Computer Administrators Group
- Locking Out an Administrator Account
- Removing Inactive Administrator Accounts
- Specifying an Administrator Account's Access Rights

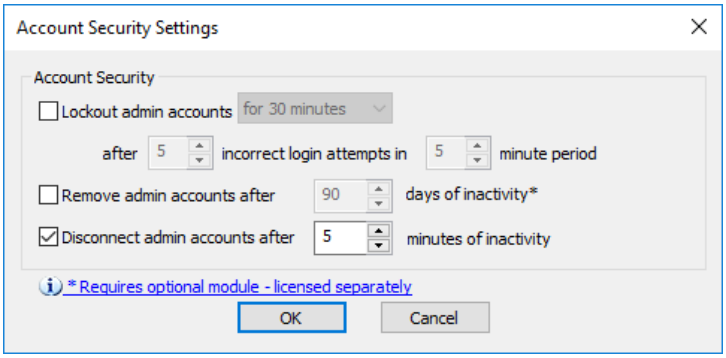
Administrator Account Security Settings Dialog Box

The **Account Security Settings**dialog box is used to unlock or lock out an administrator account, disable an inactive administrator account, change the administration interface session timeout, disable an inactive administrator account, or set up multifactor authentication for an administrator login.

To open the Account Security Settings dialog box

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure, then click the **Administration** tab.
3. Click any administrator account name (except **Local computer\administrators**), and then click **Account Policy**. The **Account Security Settings** dialog box appears.





- To lock out an account, select the **Lockout administrator accounts** check box, then specify the length of time the account is to be locked out, the number of incorrect login attempts to count, and the period during which to count the attempts. To enable an account that has been locked out, clear the **Lockout** check box.
- To remove an inactive account automatically, select the **Remove administrator accounts after**check box, then specify the number of days of inactivity after which to delete the account.
- To disable an account, select the **Disable admin account after** check box, the specify the number of days of inactivity after which to disable the account.
- To change the default administration interface session timeoutfor this administrator, select the **Disconnect administrator accounts after** check box, then specify the minutes of inactivity that you need.
- To set up multifactor authentication for an administrator account, select the **Require additional factor authentication** check box, then select **OPT - Email delivery**. Refer to Specifying Multifactor Authentication for options.

4. Click **OK** to close the dialog box.
5. Click **Apply**to save the changes on EFT.

A change in any date-sensitive value resets the calculations. For example, if this feature was configured for 60 days, and you change it to 90 days, the count resets to zero, so that any inactive account that has been inactive for 59 days and was set to be deleted tomorrow, will now not be considered inactive until 90 days from today.

Related Topics

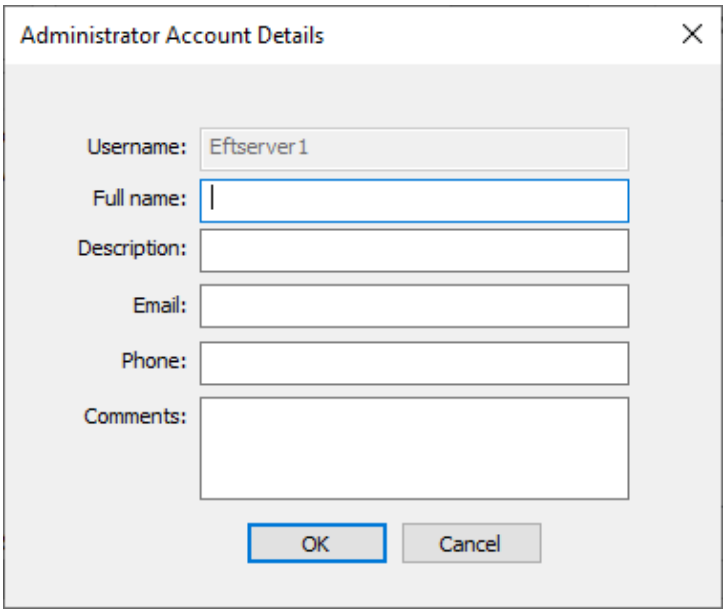
- Locking Out or Unlocking an administrator Account
- Removing Inactive administrator Accounts
- Administration Interface Session Timeout
- Administrator Account Details

Administrator Account Details

Before configuring multifactor authentication for administrator accounts, verify that each administrator account has an email address. Otherwise, EFT will not be able to email a passcode to the administrator to log in. Administrators configured for MFA via SMS without a defined mobile number will default to email address.

To add an email address or phone number to an administrator account

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure, then click the **Administration** tab.
3. Click any administrator account name (except **Local computer\administrators**), and then click **Account Details**. The **Account Details** dialog box appears.



4. Complete the fields in the dialog box:
   - **Username** - Name used for the account
   - **Full name** - First and last name of the user
   - **Description** - Type or purpose of administrator account
   - **Email** - Email address of administrator
   - **Phone** - Phone number of administrator
   - **Comments** - Other details you might want to add
5. Click **OK**, then click **Apply** to save changes.

Active Directory-Based Administration

In addition to or instead of EFT-managed administrator accounts, administrator users can authenticate via Active Directory (AD). For remote connections, the connecting account must have access to the computer on which EFT is installed. Password complexity, expiration, and so on for AD accounts are managed by the AD server rather than on EFT.

You can add Active Directory users and groups as administrator accounts and the user or group appears in the **administrator account names** list on the Server's **Administration**tab. If a user account is added to EFT only as a part of a group, the user assumes the permissions of its group. If the user is a member of multiple defined groups, the permission (role) and assignment(s) allocated to the group that provides the most privileges are assigned to that user.

An EFT administrator you should *not* be able to perform the following actions on an AD-configured user or site:

- Reset Password
- Change Password
- Rename
- Delete (although available in the EFT admin UI, but it doesn't delete the user)

An EFT administrator should be able to perform the following actions, however, they run the risk of it being overwritten when a "User Database refresh" is performed:

- Update any account details such as Name, email, phone, etc. within the "Details" tab
- Remove account as part of the inactivity cleanup

An EFT administrator should be able to perform the following user-related actions:

- Set protocols values for the user (enable/disable/overwrite/inherit)
- Set Connection Limits for the user (enable/disable/overwrite/inherit)
- Set Transfer Limits for the user (enable/disable/overwrite/inherit)
- Enable/Disable users
- Kick users
- Unlock users
- Expire users

Related Topics

- Refer to Local Computer Administrators Group for more information about accessing EFT using the administrator credentials for the local computer.
- Refer to Creating EFT Administrators for details of creating an EFT administrator account that uses AD-based authentication.

Creating EFT Administrators

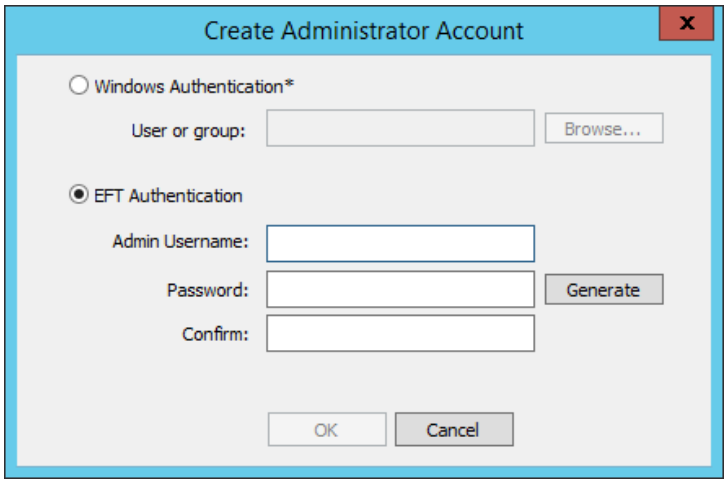
The main EFT administrator account is created when you install EFT. That account can log in and create other administrators with varying permissions. You can give other users and group access to the administrative functions of EFT by creating an administration account for them in the EFT administration interface. For security and for compliance with the PCI DSS, you should not create more than one administrator with full control over EFT. (You cannot edit the settings for your own account.) Refer to Delegated Administration for details of creating "sub" administrators with a very specific subset of permissions for managing EFT, COM, Site(s), Settings Templates, user accounts, user passwords, and reports.

While you can have two administrators working on Event Rules at the same time, if they are working on the same Rule at the same time, when they save their Rule, the second administrator to save will get a notice that the changes could not be saved because changes have been made by someone else. They then need to refresh to see the other changes, and then make their changes to the event rule again.

The administrator accounts are only used for EFT administration. If administrator users also need to log in to the Web Transfer Client to exchange files, they will need a separate user account.

To create an administrator account

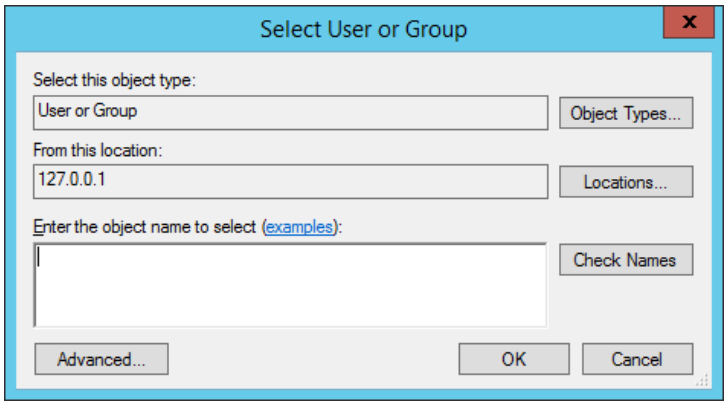
1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node to which you want to add an administrator account.
3. In the right pane, click the **Administration** tab.
4. In the **Administrator Access and Permissions**area, click **Add**. The **Create Administrator Account** dialog box appears.



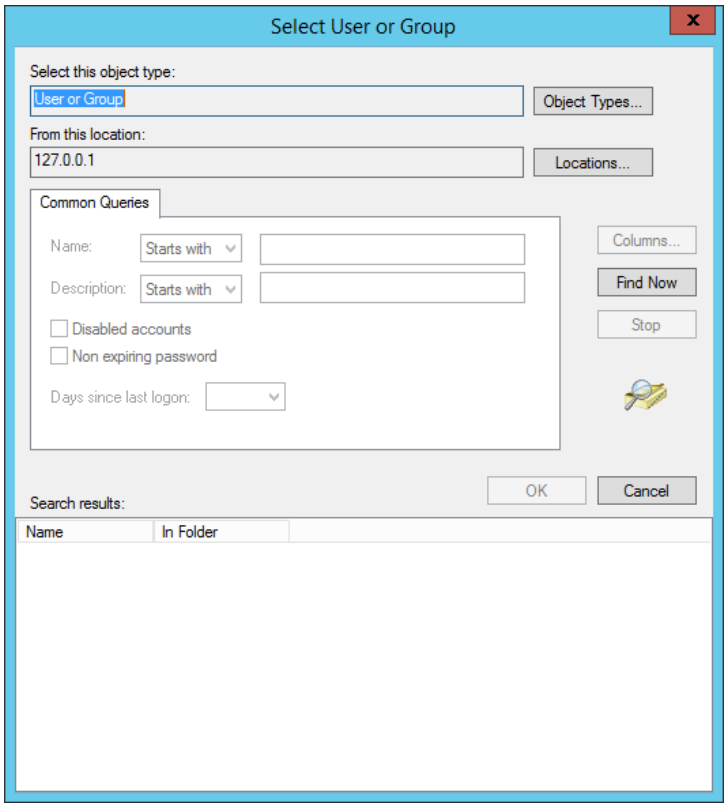
5. Specify either **Windows Authentication** or **EFT Authentication**.
    - If you choose **EFT Authentication**, specify the account details:
        a. Define a user name for the account.
        b. Define and confirm a password for the account or click **Generate**to generate a strong password.

        Passwords are case-sensitive; the username and password fields each cannot exceed 1024 characters. If the **Password**and **Confirm** boxes do not match, the **OK**button is disabled. Retype the passwords.

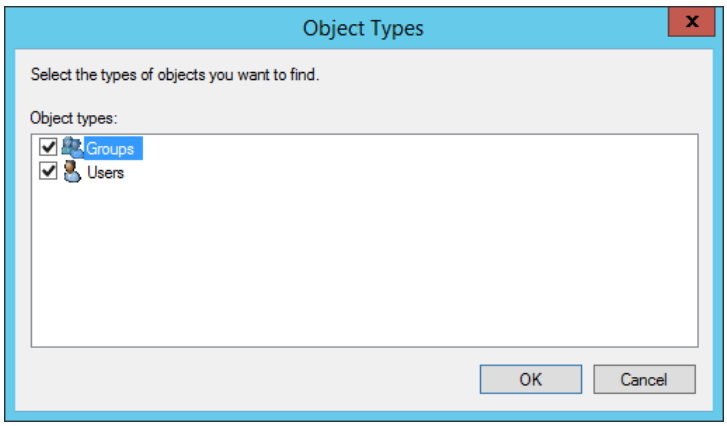
    - If you choose **Windows Authentication**, click **Browse**to specify the **User or group**. The **Select User or Group**dialog box appears.



a. To expand the dialog box, click **Advanced**.

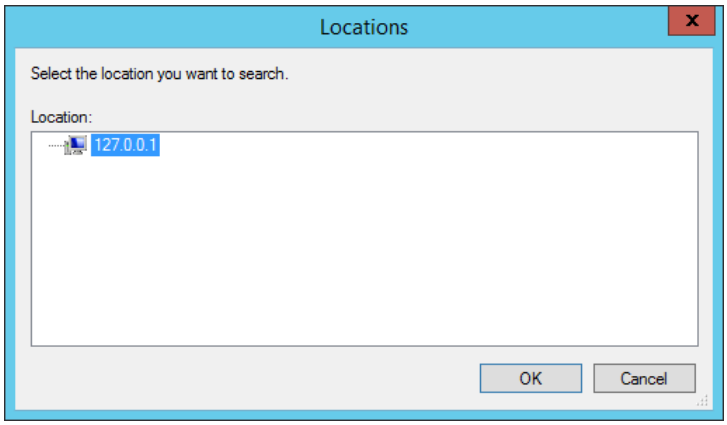


b. To specify the type of object to search for (User or Group), click **Object Types**.



c. By default, both groups and users are searched. To search only groups, clear the **Users**check box; to search only users, clear the **Group**check box, and then click **OK**.

d. Click **Locations**to specify a network address to search. The **Locations**dialog box appears with available locations displayed.

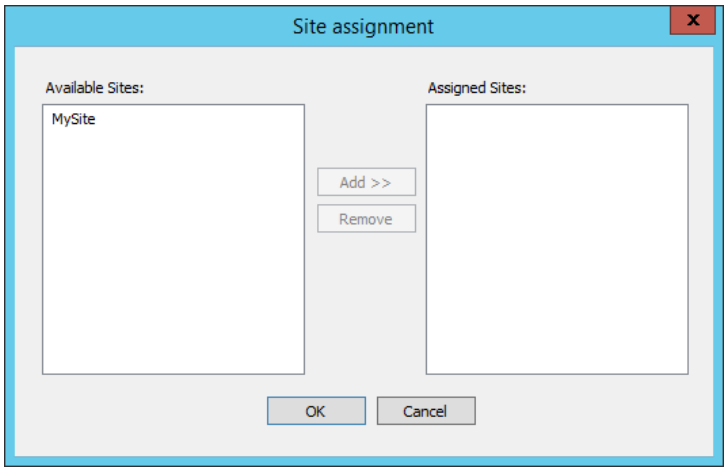


e. Click a location, and then click **OK**.
f. In the **Select User or Group** dialog box, use the **Common Queries** area to search for a specific user or group.
g. After you have specified your search criteria, click **Find Now**. The search results appear.
h. Click the user or group that you want to use for this account, and then click **OK**. The user or group appears in the **Create Administrator Account** dialog box.
i. Click **OK**.

AD accounts that are part of the local computer's administrator's group will not appear when browsing the "local computer" because these accounts are AD accounts, not local. AD accounts will appear when browsing the "AD" scope. You can select AD accounts when performing remote administration as long as the administration interface and EFT are in the same domain or working across trusted domains.

The new user appears in the **Administrator account names** box.

6. On the **Administration** tab, click the **Selected account permissions policy** box, then specify the functions this account can control. (Refer to Delegated administration for details of each type.) The**Selected account permissions policy** (Site administrator, User administrator, etc.) applies only to the account selected.
7. If you specified that the account is a Site administrator, Template Settings administrator, Change Password administrator, or User administrator, the **assignment**dialog box appears.



- Specify one or more items in the **Available**box, then double-click the selection or click **Add**, then click **OK**. The assignment appears in the **Assigned**list.

8. Complex Passwords, Password History, Password Reset, and Account Policy options apply to all EFT-managed administrator accounts defined on this Server.
9. **Optional permissions**- By default, the account has **Manage personal data**, **Run & Edit Reports**, and **COM** permissions. Clear the check box for items that you don't want to apply to the selected account.
    - **COM** - Allow or deny the administrator account to use the COM API
    - **Run & Edit Reports** - Allow or deny ability for user to run reports.
    - **Manage personal data** - Allow or deny the administrator account to manage users' personal data. Upgrading from 7.4.x enables this option on all existing administrator accounts.
10. Click **Apply** to save the changes on the Server.

Related Topics

- Changing an Administrator Password or Access Rights
- Enabling Complex Passwords for Administrator Accounts
- Enforcing Password History for Administrators
- Enforcing Password Reset for Administrator Accounts
- Expiring Administrator Passwords
- Locking Out or Unlocking an Administrator Account
- Removing Inactive Administrator Accounts
- Optional Permissions for Administrator

Administrator Account Permissions

The table below provides details of available permissions for each Administrator Account.

The **Reports**, **COM**, and **Manage Personal Data** check boxes are selected by default. Clear the check boxes if you do want to allow that access to an account.

Function	Server administrator	Site administrator	Event Rules administrator	Template Settings administrator	User administrator	Change Passwords administrator
View, create, import reports and view Reports tab	Yes, if Reports check box is selected	Yes, if Reports check box is selected	Yes, if Reports check box is selected	Yes, if Reports check box is selected	Yes, if Reports check box is selected	Yes, if Reports check box is selected
Programmatic access via COM API	Yes, if COM check box is selected	Yes, if COM check box is selected	Yes, if COM check box is selected	Yes, if COM check box is selected	Yes, if COM check box is selected	Yes, if COM check box is selected
Manage personal data	Yes, if Manage personal data check box is selected	Yes, if Manage personal data check box is selected	Yes, if Manage personal data check box is selected	Yes, if Manage personal data check box is selected	Yes, if Manage personal data check box is selected	Yes, if Manage personal data check box is selected
Add/delete/edit Server Groups	Yes	No	No	No	No	No
View Server node	Yes	No	No	No	No	No
Add, delete, edit Servers	Yes	No	No	No	No	No
Stop/start/modify Server service	Yes	No	No	No	No	No
View Server statistics (General tab)	Yes	No	No	No	No	No
Access the PGP, SFTP, and SSL> key manager, and create, import, export, and add keys and certificate	Yes	Yes	Yes, within Event Rules	Yes	No	No

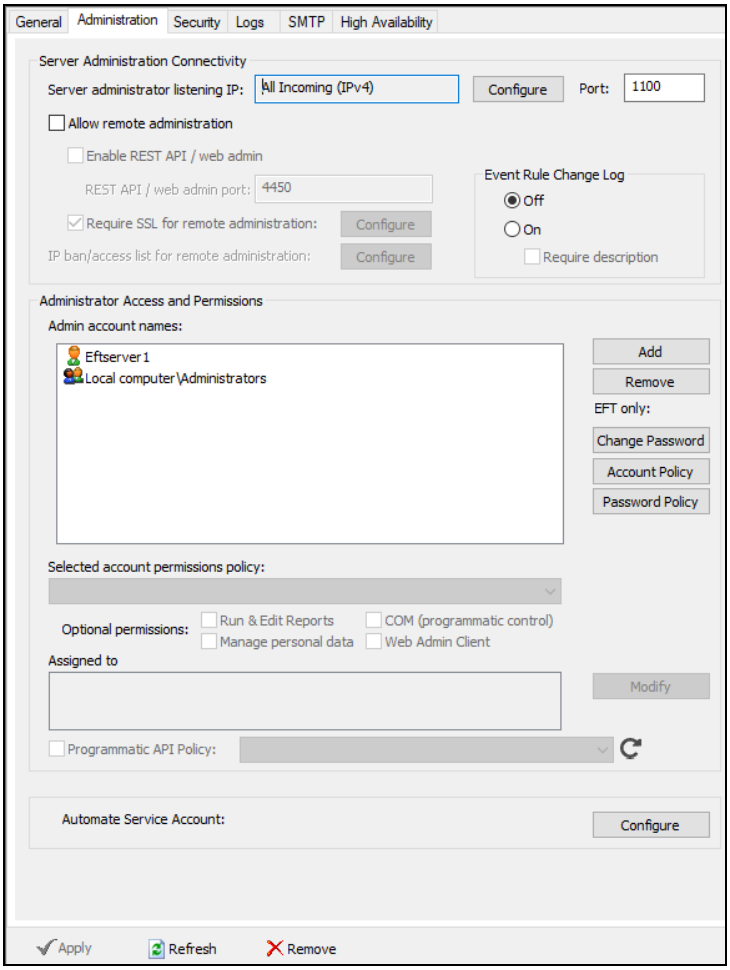
Function	Server administrator	Site administrator	Event Rules administrator	Template Settings administrator	User administrator	Change Passwords administrator
Delete keys or certificates	Yes	No	Yes, within Event Rules	No	No	No
View Status tab	Yes	Yes	Yes	Yes	No	No
Add/Delete/Edit Sites	Yes	No	No	No	No	No
View Site node	Yes	Yes	Yes	No	No	No
Stop/Start Sites	Yes	Yes, for the assigned Site(s)	No	No	No	No
Add, delete, edit administrator accounts (including change passwords)	Yes	No	No	No	No	No
Add, delete, edit Settings Templates	Yes	Yes	No	No	No	No
View Settings Templates node	Yes	Yes	Yes	No, just the assigned Settings Template	No	No
Enable/Disable users	Yes	Yes, for the assigned Site(s)	No	Yes, for the assigned Settings Template(s)	Yes	Yes
Unlock a user account that was locked from too many failed login attempts	Yes	Yes, for the assigned Site(s)	No	Yes, for the assigned Settings Template(s)	Yes	Yes
Change user passwords	Yes	Yes, for the assigned Site(s)	No	Yes, for the assigned Settings Template(s)	Yes	Yes
Add users	Yes	Yes, for the assigned Site(s)	No	Yes, for the assigned Settings Template(s)	Yes	No

Function	Server administrator	Site administrator	Event Rules administrator	Template Settings administrator	User administrator	Change Passwords administrator
Delete users	Yes	Yes, for the assigned Site(s)	No	Yes, for the assigned Settings Template(s)	No	No
View, change users' settings	Yes	Yes, for the assigned Site(s)	No	Yes, for the assigned Settings Template(s)	No	No
Kickand monitor users	Yes	Yes, for the assigned Site(s)	No	Yes, for the assigned Settings Template(s)	No	No
View VFStab	Yes	Yes, for the assigned Site(s)	Yes	Yes	No	No
Modify VFS tree	Yes	Yes, for the assigned Site(s)	No	Yes, for the assigned Settings Template(s)	No	No
Change VFS root path for assigned Settings Templates	Yes	No	No	No	No	No
View Groups node	Yes	Yes, for the assigned Site(s)	Yes	No	No	No
View, modify Group assignments	Yes	Yes, for the assigned Site(s)	Yes	Yes, for the assigned Settings Template(s)	No	No
View Commands node	Yes	Yes, for the assigned Site(s)	Yes	No	No	No
View Event Rules node	Yes	Yes, for the assigned Site(s)	Yes	No	No	No
View Advanced Workflows node	Yes	Yes, for the assigned Site(s)	Yes	No	No	No

Function	Server administrator	Site administrator	Event Rules administrator	Template Settings administrator	User administrator	Change Passwords administrator
View Gateway node	Yes	Yes, for the assigned Site(s)	Yes	No	No	No

Optional Permissions for Administrator

On the **Server > Administration**tab, you can add and remove optional permissions for a selected administrator account.



The optional permissions include:

- **Run & Edit Reports**- Allows the selected administrator account to run and edit reports
- **COM (programmatic control)**- Allows the selected administrator account to use COM API objects to manage EFT
- **Manage personal data**- Allows the selected administrator to manage user account information. An administrator user without permission to **Manage personal data** can view personal data in the EFT Logs. Remote administrators cannot see the logs.

- **Web Admin Client** - Allows selected admin account to use the Web Admin Client. (This is NOT selected by default.) If the **Web Admin Client** check box is selected, the **Programmatic API Policy** checkbox/dropdown will become enabled, greyed out, with "use account permission policy" selected. If you try to use the Web Admin Client without **Web Client Access** selected, you should get an error in the Web Admin Client.
- **Programmatic API Policy** - Used to apply full or read-only access to a selected administrator account when **Enable REST API** is selected. Other permissions can be configured in the PermissionRoles.json file. If the **Web Admin Client** check box is selected, the **Programmatic API Policy** checkbox/dropdown will become enabled, greyed out, with "use account permission policy" selected.

Each of these options is enabled by default and independent of the account permissions policy selected (that is, delegated administrators).

Related Topics

- Creating EFT Administrators
- Account Security Settings Dialog Box
- Administrator Account Permissions
- Delegated Administration
- Changing an Administrator Password

Specifying Administrator Account's Access Rights

Anyone with Server Administrator rights can modify other administrator accounts. If you have only one server administrator account and you have forgotten the password, refer to Resetting the EFT Administrator Password.

To modify an administrator account

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node on which the administrator account is defined.
3. In the right pane, click the **Administration**tab.
4. In the **Administrator Account Names** list, click the account that you want to change.
    - To change the delegate options, refer to Adding Server Administrators.
    - To change account security settings, refer to Deleting Inactive Administrator Accounts and Locking Out an Administrator Account.
5. Click **Apply** to save the changes on EFT.

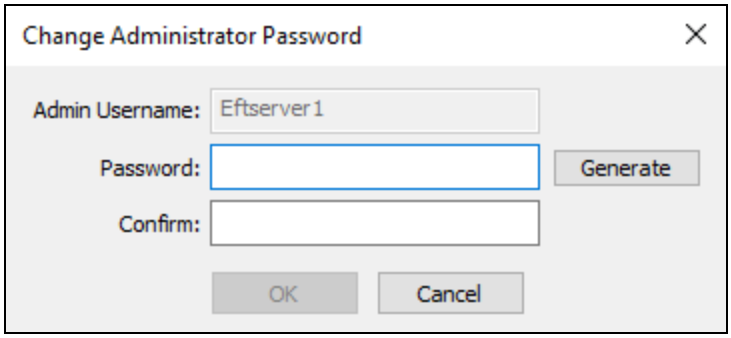
Changing an Administrator Password

Anyone with Server administrator rights can modify administrator accounts.

If you have only one server administrator account and you have forgotten the password, refer to Resetting the EFT administrator Password.

To modify an administrator account

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node on which the administrator account is defined.
3. In the right pane, click the **Administration**tab.
4. In the **Administrator Account Names** list, click the account that you want to change.
5. Click **Change Password**. The **Change Administrator Password Account** dialog box appears.
6. Define and confirm a password for the account or click **Generate** to generate a strong password. (If you click **Generate**, the password is visible in this dialog box.)

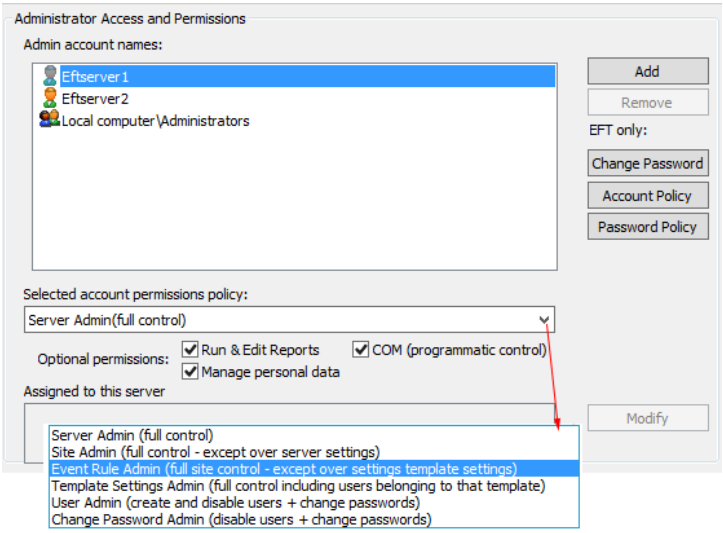


   - Passwords are case-sensitive.
   - Passwords can be a minimum of 12 characters, but default to 15 characters to meet regulatory compliance standards.
7. Click **Apply** to save the changes on EFT.
   - To change the delegate options, refer to Adding Server administrators.
   - To change password security settings, refer to Enforcing Complex Passwords for Administrator Accounts, Enforcing Password Reset for Administrator Accounts, and Expiring Administrator Passwords.

- To change account security settings, refer to Removing Inactive Administrator Accounts and Locking Out an Administrator Account.

Delegated Administration

EFT allows you to assign *sub* administrator accountsthat have a very specific subset of permissions for managing EFT, COM, Site(s), Settings Templates, user accounts, user passwords, and reports. Permissions are assigned to sub-administrators via a series of controls on the server's **Administration**tab.



For example, suppose you want to give your help-desk people the ability to create user accounts on EFT, but you are worried that the help-desk might accidentally make changes to EFT in the process of creating these accounts. Furthermore, you do not want the help desk people to manage user accounts that belong to the engineering and marketing groups. Delegated administration allows you to create one or more sub-administrator accounts that have access ONLY to user accounts management. Using templates to house marketing, engineering, and other department accounts, you can further limit the sub-administrators to only those accounts for departments that they are authorized to manage. Also, each of the sub accounts can be allowed or denied access to COM and/or Auditing and Reporting.

All administrator accounts are treated equally with respect to password expiration, reset, and removal of inactive accounts.

If you change the Event Rule permissions (such as whether a user can read from, write to, or execute a rule) for an administrator when they are logged in to the administration interface, the account user will have to log out and then log back in to effect the changes.

(See also Optional Permissions for administrator.)

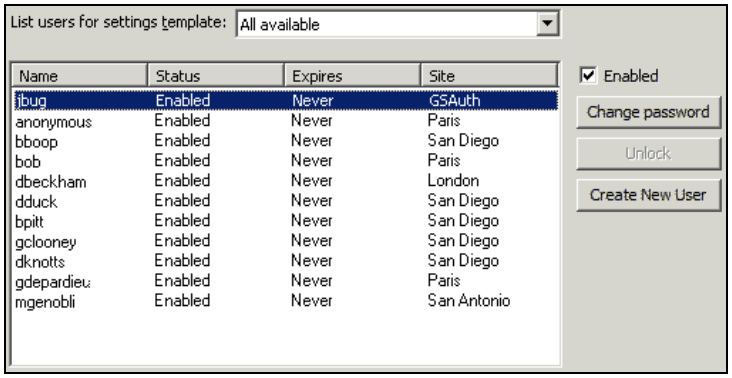
The available sub administrator account types include:

- **Server administrator -** Can create, modify, or remove administrator accounts, and can manage Sites, Settings Templates, and user accounts.
- **Site administrator -** Can manage everything for a specific Site and the Settings Templates on the Site, and can change user passwords, but does not have control over EFT. The Site administrator cannot click the **Server** node nor access any of the node's tabs; stop/start the Globalscape Server service from within the administration interface; create, remove, or rename Sites, Servers, or Server Groups; access or modify EFT global or applet settings; close the Server engine; or stop/start any Site other than those assigned to the Site administrator.
- **Event Rule administrator** - Similar to Site administrator, but more restrictive. Cannot manage Groups, Settings Templates, Transfer Activity, or Gateway tab. The Event Rule administrator can view and manipulate within Event Rules the VFS, HA nodes for load balancing, address book, OpenPGP keys, Report names, users, Settings Template names, Group names, Backup, Content Integrity profile names, AS2 profile names, calendar names, Email Actions, context variables. The Event Rule administrator must be given explicit permission to manage Event Rules and Connection Profiles; the default is all permissions.
- **Template Settings administrator -** full control over the accounts assigned to that Settings Template, including the ability to view, add, remove, and modify user accounts, and group assignment; can change all Settings Template settings, except for the VFS root path for assigned Settings Templates; can see the entire VFS tree, but can only modify the parts of the VFS that belong to root folders that belong to the Settings Template to which the account is assigned; can access the **General**tab on EFT to view statistics; can kick and monitor users.

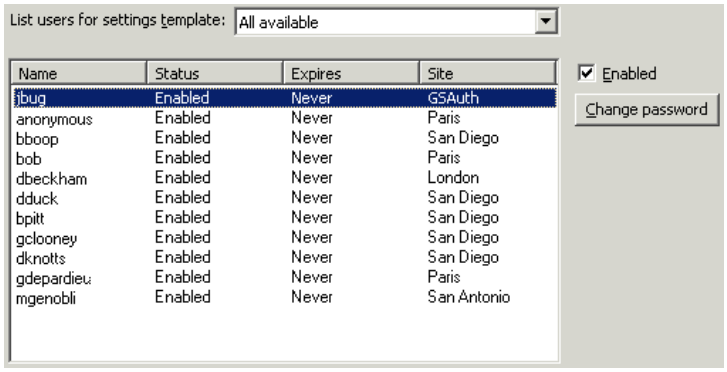
  They cannot access the **Reports** tab unless specifically allowed; cannot select the **Site**, **Server**, or **Server Group** nodes, nor view the corresponding tabs; cannot access Server settings, nor any Settings Template not assigned to their account. They can access the OpenPGP, SFTP, and SSL key manager, and create, import, export, and add keys and certificates. They cannot delete keys or certificates.
  - A Template Settings administrator is not permitted to change the Settings Template home (root) folder that was assigned by the Site or Server administrator.
  - A Template Settings administrator is not permitted to change the value of the "Treat home folder as user's default root folder" setting.

- When creating or modifying users, the Template Settings administrator cannot browse or manually designate paths relative to the Settings Template root folder.
- A Template Settings administrator can delete users and, consequently, the user's home and sub-folders, as long as the user belongs to a template assigned to that administrator, and that user's root folder is subordinate to the Settings Template root folder.

- **User administrator**- Has all the privileges of the Change Password administrator, but can also create new users. The User administrator is not allowed to see or edit users' settings or Template settings, and is limited to change password, disable user, or create more users. User administrators can unlock user accounts.



- **Change Passwords administrator -** Can enable/disable users and change passwords for users in their specified Settings Template(s), but cannot add nor remove users, manage other Settings Template(s), manage Sites, nor control EFT. When a Change User Password administrator logs in to EFT, only the view below is available.



Related Topics

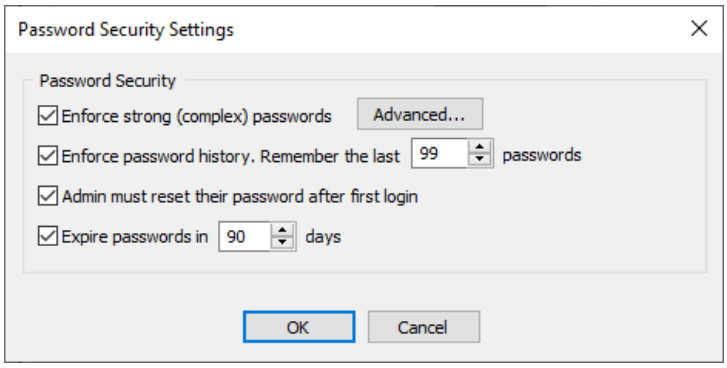
- Adding EFT Administrators
- Changing an Administrator Password or Access Rights
- Configuring Server Administrators
- Administrator Account Permissions

Enforcing Complex Passwords for Administrator Accounts

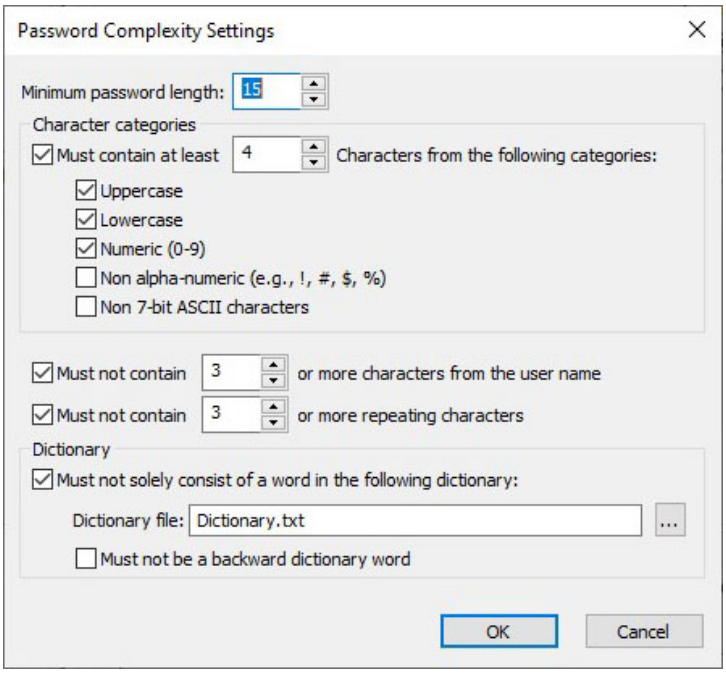
When you create or edit EFT-managed administrator accounts, you can specify that all administrator accounts be required to adhere to certain password complexity rules.

To set complexity settings for administrator accounts

1. Refer to Adding EFT Administrators or Changing an Administrator Password or Access Rights for the procedures for creating or changing an administrator account.
2. In the administration interface, connect to EFT and click the **Server** tab.
3. On the **Server**tab, click the Server node to which you want to add an administrator account.
4. In the right pane, click the **Administration** tab.
5. Click an EFT-managed administrator account, then click **Password Policy**. The **Password Security Settings** dialog box appears.



6. Select the **Enforce strong (complex) passwords** check box to ensure that when any administrator creates or changes a password for any administrator account, password complexity is enforced.
7. To specify password complexity settings, click **Advanced**. The **Password Complexity Settings** dialog box appears.



8. In the **Minimum password length** box, specify the minimum number of characters the password must contain. The minimum for EFT is 12 characters. The default is set to 15 characters.
9. In the **Must contain at least** box, specify the number of characters from the following categories: **Uppercase**, **Lowercase**, **Numeric (0-9)**, **Non-alphanumeric (for example, !, #, $, %)**, and **Unicode**. Select the check boxes for the applicable characters. (Certain non-alphanumeric characters might not be available when using a mix of English and non-English language settings and keyboards.)
10. In the **Must not contain** boxes, select the check boxes and specify the number of characters from the user name and/or number of repeating characters the password must not contain.
11. In the **Dictionary** area, select the **Must not solely consist of a word in the following dictionary**, then specify the dictionary file. A default dictionary file is provided in EFT installation directory.
12. Select the **Must not be dictionary word backwards** to ensure the password is not a word in the dictionary file spelled backward.
13. Click **OK**to close the **Password Complexity Settings** dialog box.
14. Click **OK** to close the **Password Security Settings**dialog box.
15. Click **Apply**to save the changes on EFT.

Field	Default	Min/Max Values
Minimum password length - Specify the minimum number of characters that must be in the password	15	6 - 99

Field	Default	Min/Max Values
In the **Character categories**area, specify the type of characters that must be in the password: The password must contain characters from at least N of the following categories: • Uppercase • Lowercase • Numeric (0-9) • Non alpha-numeric (for example, !, #, $, %) • Unicode (UTF-8)	3 categories	2 categories, up to the maximum password length
Must not contain N or more characters from the user name	3	2 characters, up to maximum password length
Must not contain N or more repeating characters.	3	2 characters, up to maximum password length
Must not consist solely of a word in the following Dictionary file. (Click the ellipse icon to select a file.)	on	n/a
Must not be a dictionary word backwards	off	n/a

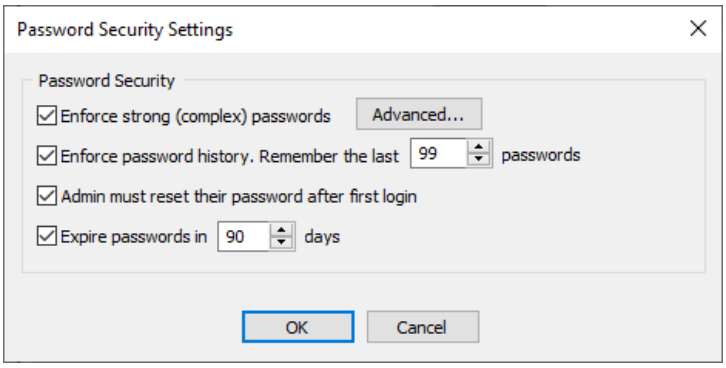
If anyone tries to change a strong administrator password to a password that does not meet the specifications in the **Password Complexity Settings** dialog box, an error message appears.

Enforcing Password History for Administrators

You can enable EFT to remember the previous passwords of administrator accounts so that administrators must create unique passwords.

To configure administrator accounts to enforce password history

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure.
3. In the right pane, click the **Administration**tab.
4. Click an EFT-managed administrator account, and then click **Password Policy**. The **Password Security Settings**dialog box appears.



5. Select the **Enforce password history** check box, then specify the number of passwords to remember. The default is 4.
6. Click **OK** to close the dialog box.
7. Click **Apply**to save the changes on EFT.

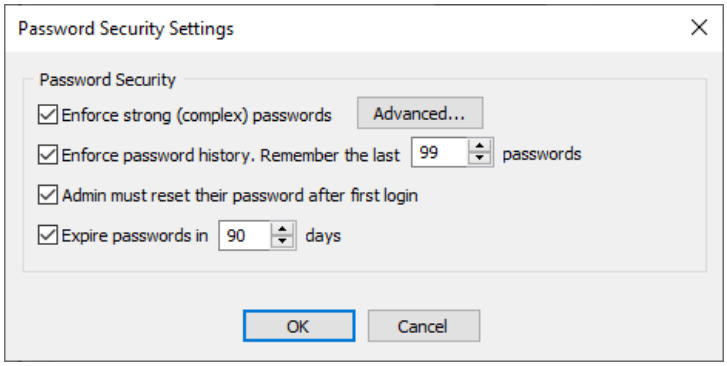
Enforcing Password Reset for Administrator Accounts

EFT provides the option to force administrators to change their password on log in. On Sites defined using the "strict security settings," users are forced to change their passwords on first use.

You can enable the password reset page while disallowing general access to HTTP or HTTPS. When a new user logs in to EFT via the HTTP or HTTPS index page, EFT redirects the user to the reset page. After the user creates a new password, they are returned to the index page.

To configure administrator accounts to enforce password reset

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure.
3. In the right pane, click the **Administration**tab.
4. Click an EFT-managed administrator account, then click **Password Policy**. The **Password Security Settings** dialog box appears.



5. Select the **Admin must reset their password after first login** check box. Administrators are prompted to change their password when they log in to the Site.
6. Click **OK** to close the dialog box.
7. Click **Apply**to save the changes on EFT.

When a password is reset, EFT verifies the new password against complexity criteria and password history, if those features are enabled. The administrator is not allowed to proceed with the session until a password is created and accepted by the system. If the password is not accepted by the system:

- In HTTPS and SFTP, the authentication request will be denied.
- In FTP, no further FTP commands will be accepted until the new password is provided and meets complexity and password history requirements, if those features are enabled.

For high security-enabled (strict security) Sites:

- PCI DSS requirements state that you should set first-time passwords to a unique value for each user and force users to change their password immediately after the first use.
- A warning appears if you clear the **administrator must reset their password after first login** check box. If an administrator logs in using a temporary password, a warning appears to prompt the administrator to supply a new password.
- Passwords should be reset every 90 days.

EFT cannot ask FTP users to change their password prior to logging in and identifying themselves. EFT allows them to login (authenticate), but then prevents any further interaction until they change their password.

Specifying Multifactor Authentication for Admin Accounts

EFT supports multifactor authentication (MFA) for administrator accounts. (This is also a requirement for PCI DSS 4.0.1 compliance.) This is similar to the MFA in the **File send** dialog box for the Send and Reply portals, and on the **Site > Connections** tab for the WTC and Workspaces.

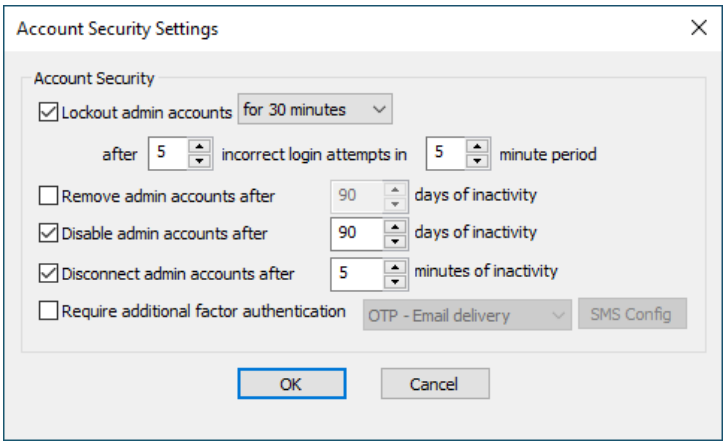
How does MFA work in EFT?

1. When logging in to the admin interface, if the **Require additional factor authentication** check box is selected and configured (shown below), EFT prompts for a passcode, and informs the recipient to check their email or text messages.
2. EFT generates a OTP and sends it in an email or text message to the recipient. (The user account details must include their mobile phone number to use SMS; otherwise the email address is used. Therefore, for ad hoc interactions, you should specify email delivery of the OTP.)
3. The recipient checks email/text, and copies the passcode to the clipboard (or clicks the link).
4. The recipient pastes the passcode (or follows link) into the prompt.
5. If the passcode is verified, EFT allows access.

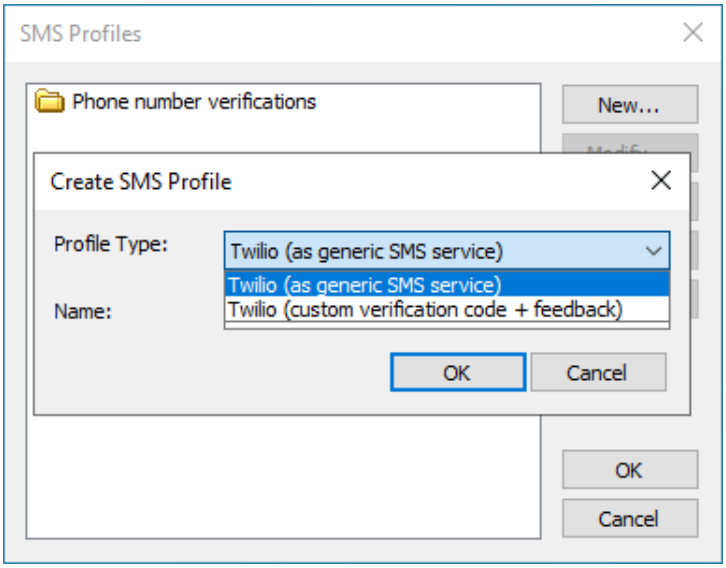
IMPORTANT: Be sure each account has an email address specified so that no one is locked out of their account when MFA is enabled. Otherwise, EFT will not be able to email the passcode to log in. Refer to **Account Details for Admins** to provide email addresses and phone numbers to administrator accounts.

To set up multifactor authentication for an administrator account

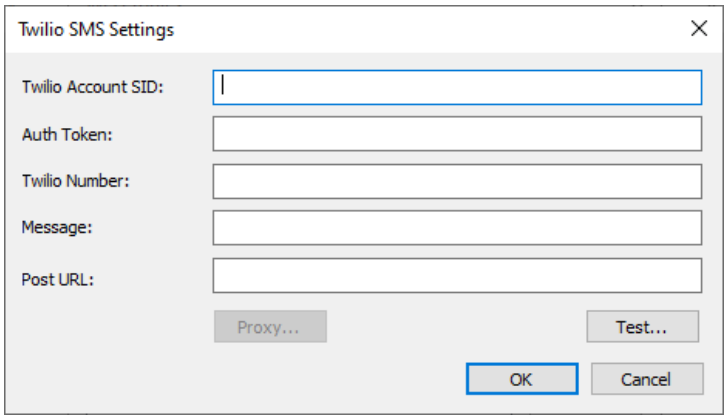
1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure, then click the **Administration** tab.
3. Click any administrator account name (except **Local computer\administrators**), and then click **Account Policy**. The **Account Security Settings** dialog box appears.

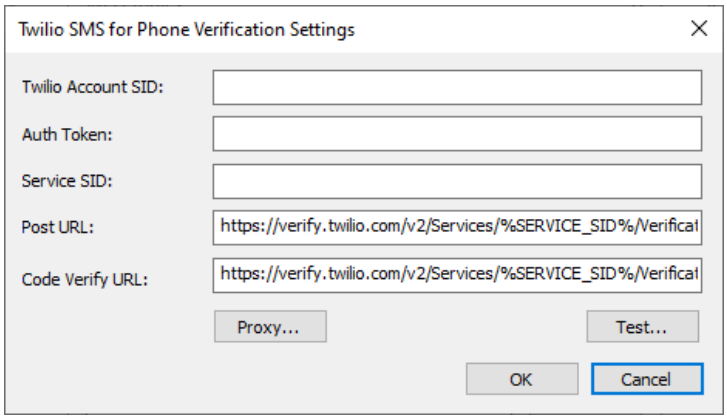


4. Select the **Require additional factor authentication** check box, then select **OPT - Email delivery**.
5. In the **OTP -Email delivery** drop-down list, choose **OTP - Email Delivery**, **SMS Delivery**, or **try SMS then email**.
6. If you chose **SMS Delivery** or **OTP - try SMS then email**, click **SMS Config**, to open the SMS profiles dialog box.
7. Click **New** to create a new profile. The **Create SMS Profile** dialog appears.



8. In the **Profile Type** list, specify either **Twilio (as generic SMS service)** or **Twilio (custom verification code + feedback)** then click **OK**. Depending on which one you chose, the **Twilio SMS Settings** or the **Twilio SMS for Phone Verification Settings** dialog box appears.





a. Provide the **Twilio Account SID** copied from your Twilio account.
b. Provide the **Auth Token** copied from your Twilio account.
c. Provide the **Twilio Number** copied from your Twilio account. You must include the country code and the + PLUS SIGN (that is, in the USA, +1) in front of the number.
d. Provide the **Message**that will be sent in the SMS, but keep the variable `%Account_Session_OTP%`. This variable is used by EFT to send the OTP. Do not edit anything between the percent symbols.
e. Provide the **Post URL** copied from your Twilio account.
f. Configure a **Proxy**, if needed. Refer to Defining a Proxy for details.
g. Click **Test** to verify the connection.
h. If the test is successful, click **OK**.

9. Click **OK** to close the **SMS Profiles** dialog box.
10. Click Apply to save your settings.

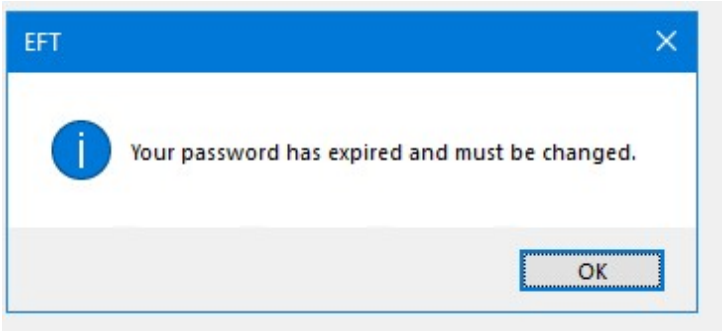
Expiring Administrator Passwords

If **Expire Passwords** is enabled and a user logs in with an administrator account with a temporary password, EFT prompts the user to supply a new password. Each day it also checks whether passwords are <n> days from expiration, and those passwords are flagged for reminders, if reminders are enabled. All reminder email messages are sent immediately after flagging the accounts to be reminded.

EFT executes cleanup procedures every day at 00:00:00 UTC and at Server Startup. This daily server cleanup removes/disables inactive administrators and user accounts and sends password reset and expiration notifications for every Site.

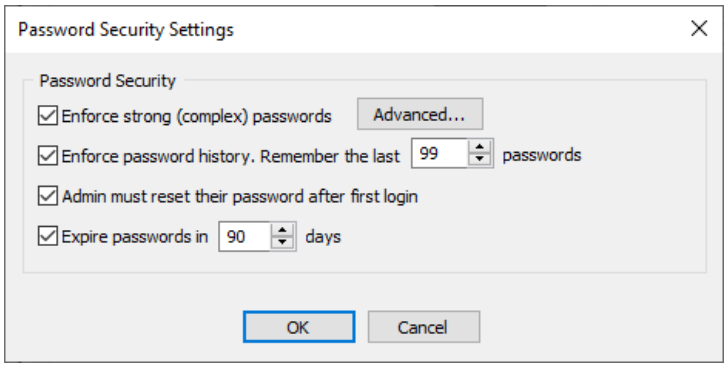
EFT cannot ask FTP users to change their password prior to logging in and identifying themselves. EFT allows them to login (authenticate), but then prevents any further interaction with their session until they change their password.

NOTE: For PCI DSS compliance, administrator account passwords must be changed every 90 days. When you attempt to log in with an expired password, a message appears to tell you to change your password.



To expire administrator account passwords

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node you want to configure.
3. In the right pane, click the **Administration**tab.
4. Click an EFT-managed administrator account, then click **Password Policy**. The **Password Security Settings** dialog box appears.



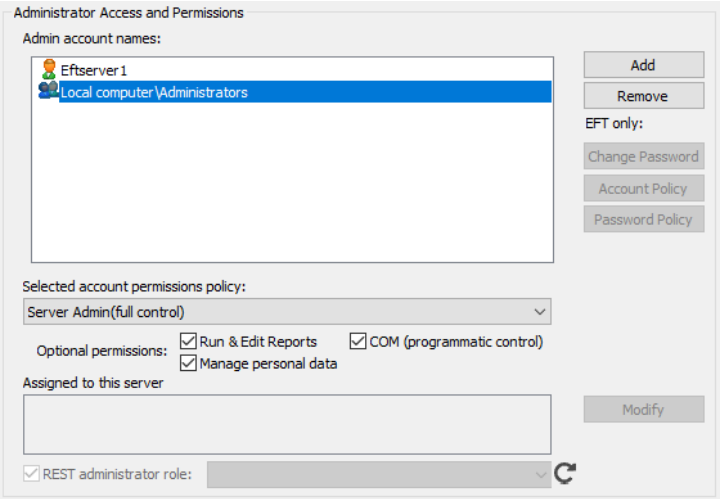
5. To specify the number of days after which to disable or remove administrator accounts, select the **Expire passwords** check box, then type or use the arrows to specify the number of days. The default is 90 days. (In EFT v8.3 and later, this check box is selected by default.)

   If you make any changes to the password settings, when you click **Apply** to push the changes to EFT, the counter is reset. For example, if you set it for 90 days, then go back 89 days later and specify a different dictionary file, when you click **OK** then **Apply**, the administrator accounts will not expire for 90 days.

6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

Local Computer Administrators Group

For new installations (not upgrades) EFT queries the computer's local administrators group and adds that group to EFT's administrator account name list with the one local administrator group object, and assigns the administrator group object Server-level permissions. The **Local computer\Administrators**group object allows you to log in to EFT using the administrator credentials for the local computer. You cannot change the group's permissions when you are logged in as a user in that group.



- Refer to Active Directory-Based administration for more information about accessing EFT using the Active Directory accounts.
- Refer to Adding Server administrators for details of creating an EFT administrator account that uses AD-based authentication.

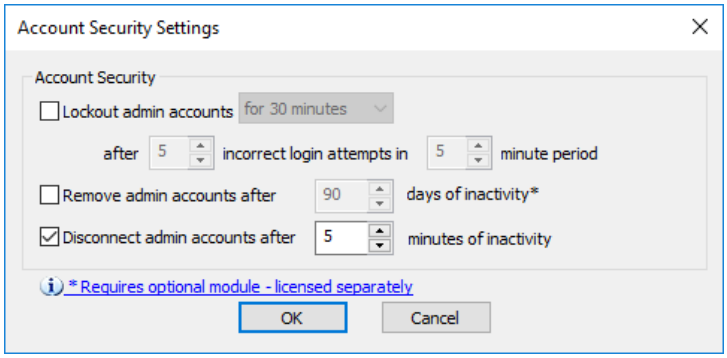
Locking Out an Administrator Account

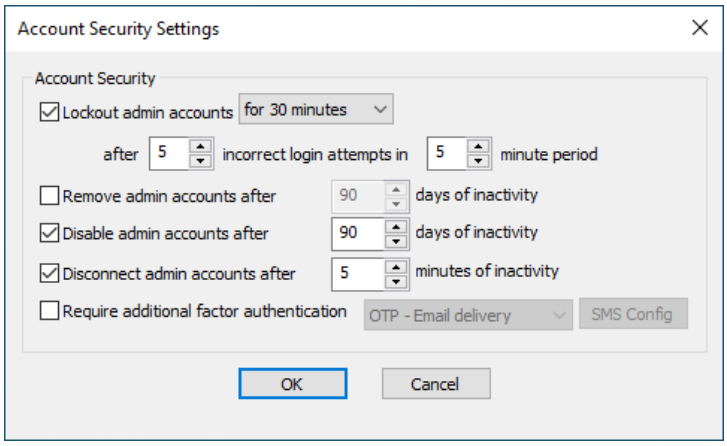
EFT can automatically lock out an administrator account after a specified number of incorrect login attempts over a specified time.

Instruct administrators regarding the timeout setting, after which they can try to log in again. If they are unable to wait for the lockout to timeout, use the procedure below to enable the account.

To disable or remove an account after a defined number of incorrect login attempts

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure, and then click the **Administration** tab.
3. Click an EFT-managed administrator account, then click **Account Policy**. The **Account Security Settings** dialog box appears.





4. Select the **Lockout administrator accounts** check box, then specify the length of time the account is to be locked out, the number of incorrect login attempts to count, and the period during which to count the attempts.

- For PCI DSS/ high-security Sites, after a maximum of 10 unsuccessful login attempts, the account should be locked out for at least 30 minutes or until they verify their identity through the help desk or other means.

5. Click **OK** to close the dialog box.
6. Click **Apply**to save the changes on EFT.

To enable an account that has been locked out

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure, and then click the **Administration** tab.
3. Click the EFT-managed administrator account that is locked, and then click **Account Policy**. The **Administrator Account Security**dialog box appears.
4. Clear the **Lockout** check box.
5. Click **OK** to close the dialog box.
6. Click **Apply** to save the changes and enable the locked out account.

Related Topics

- Removing Inactive administrator Accounts
- Expiring administrator Passwords
- Possible PCI Compliance Report Outcomes

Removing Inactive Administrator Accounts

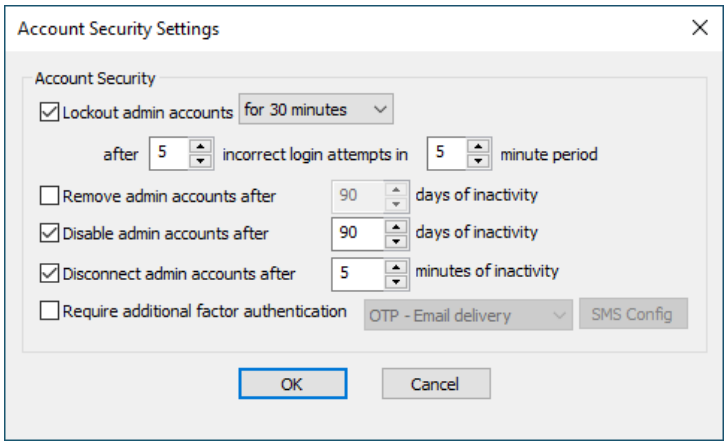
EFT executes cleanup procedures every day at 00:00:00 UTC and at service startup. This daily server cleanup removes/disables inactive administrators and user accounts and sends password reset and expiration notifications for every Site.

For Sites defined using the "strict security settings," EFT enables the option to disable or remove inactive accounts automatically, and warn if you attempt to disable that setting. The option to remove administrator accounts will be enabled by default, unless during the setup process you choose not to enable this option. EFT prompts administrators when they login advising them of the potential removal of their account if their login failed due to unknown login name. The removal of accounts is captured in the Auditing and Reporting database for reporting.

If a user attempts to log in remotely to EFT with an administrator username that does not exist or an incorrect password, a warning message appears in the administration interface.

To disable an administrator account

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure, and then click the **Administration** tab.
3. Click any administrator account name (except **Local computer\administrators**), and then click **Account Policy**. The **Account Security Settings** dialog box appears.



4. Click the administrator account that you want to disable, then click **Disable admin account after *n* days of activity**.
5. Click **OK** to close the dialog box, then click **Apply**.

To remove an administrator account

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure, and then click the **Administration** tab.
3. Click the administrator account that you want to delete, then click **Remove**. A warning prompt appears.
4. Click **Yes**, then click **Apply**.

To specify automatic deletion of inactive administrator accounts

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Server node you want to configure, and then click the **Administration** tab.
3. Click an EFT-managed administrator account, then click **Account Policy**. The **Account Security Settings** dialog box appears.
4. Select the **Remove administrator accounts after** check box, then specify the number of days of inactivity after which to delete the account.
5. Click **OK** to close the dialog box.
6. Click **Apply**to save the changes on EFT.

A change in any date-sensitive value resets the calculations. For example, if this feature was configured for 60 days, and you change it to 90 days, the count resets to zero, so that any inactive account that has been inactive for 59 days and was set to be deleted tomorrow, will now not be considered inactive until 90 days from today.

Resetting the EFT Administrator Password

If you have multiple EFT administrator accounts and need to reset one of them, refer to Changing an Administrator Passwordinstead of the procedure below.

You can define multiple EFT administrator accounts in EFT, and any server administrator account can edit another. What do you do if you have only one server administrator account and you forget the password? You can reset it using the procedure below. However, you will lose all user- and group-specific settings. The user accounts and their folder structures will remain, but permissions and settings will be lost.

Be sure to back up any other files in EFT installation folder that you will need, such as certificates. Refer to Backing Up or Restoring Server Configuration.

To reset the administrator username and password (if there are no other administrator accounts from which to access EFT)

1. Stop the EFT service.
2. Navigate to the EFT installation folder (for example, **C:\ProgramData\Globalscape\EFT Server**).
3. Using the Windows **Add/Remove Programs** utility, uninstall EFT.
4. Reinstall EFT.
5. Create a new administrator username and password.
6. Open the administration interface and login with your new username and password.
7. Recreate your Site(s) with the same name(s), EXACTLY as you used previously. The Site name must match character for character.
8. Stop the EFT service.
9. Restart the EFT service and log in. The individual groups and user accounts should be preserved; however, you must reassign permissions and settings.

Server Configuration

This section provides information regarding EFT server configuration in the administration interface.

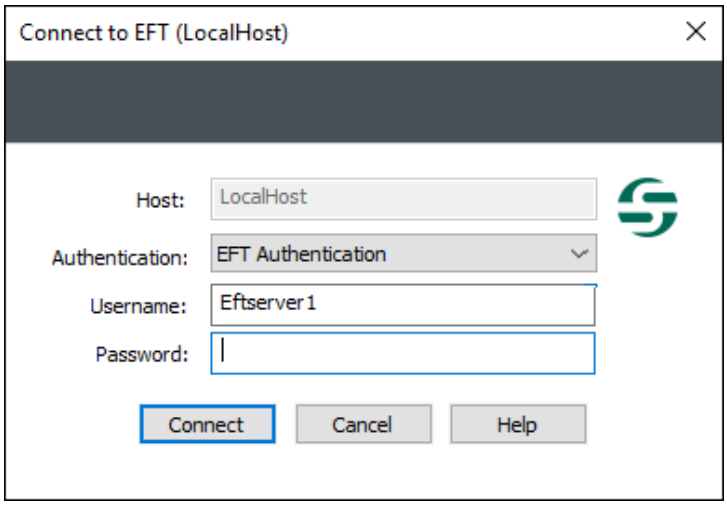
- Logging In to Administer EFT
- Logging Out of EFT in the Administration Interface
- Starting and Stopping EFT
- Command-Line Login
- Listening IP Address and Port
- Specify the Default Time Stamp
- Deregister Licenses
- Administering the Server Service
- Advanced Properties
- Email Server Settings (Includes Microsoft 365 OAuth and Google Cloud OAuth)
- Extending the Trial
- Connection Problems
- Specifying a New Local or Remote EFT
- New Remote EFT Administration Connection
- Server Groups
- Renaming, Deleting, and Moving a Server
- Monitoring Connections to EFT
- EFT Messages and Templates
- File Locations
- Encryption Algorithms
- Old Algorithms Removed
- IPv6 Support in EFT
- IDN Support in EFT
- Erasing EFT Configuration

Logging In to Administer EFT

You can log in to EFT locally or remotely (if configured) via the EFT administration interface, via the COM API, at a command line, or using a Windows shortcut. This topic discusses logging in via the administration interface. These instructions assume that EFT has been configured and the EFT service is running. For instructions for installing a remote administration interface, refer to Installing the administration Interface Remotely.

To log in to EFT

1. Do one of the following:
    - Open the administration interface. The **EFT Server administrator Login** dialog box appears.
        a. If you are logging in to the local computer, leave **This computer** selected.
        b. If you are logging in to a remote computer, click **A remote computer**, then specify the remote host.
    - If the administration interface is already open, click the Server object in the tree or the Connect icon. The **Connect to EFT**dialog box appears. The **Host**box displays the EFT name.



2. Click the **Authentication**box and specify the type of authentication to use for this login. Future connections will default to the authentication type that you specify during this initial login, but you can choose a different type. Authentication types include:
    - **EFT Authentication**- Choose this option to log in with an EFT-specified administrator account.
    - **Currently Logged On User** - Choose this option to log in as the currently logged on user (Integrated Windows Authentication).
    - **Windows Authentication**- Choose this option to log in with a specific Windows account.
3. When logging in with **EFT Server Authentication** or **Windows Authentication**, in the **Username**and **Password** boxes, provide the login credentials that you created during installation, and then click **Connect**.
    - If you have not activated your serial number and you are in the trial period, click **Continue** on the **Welcome**page.
    - If you have not activated your serial number and the trial has ended, click **Developer Mode** on the **Welcome**page.

    If your login fails, make sure you've selected the corrected authentication type.

Logging Out of EFT in the Administration Interface

EFT incorporates an internal timeout that applies to connections to EFT via the administration interface. A warning message and countdown timer appear after 10 minutes of inactivity. To change this timeout, refer to Administration Interface Session Timeout.

To log out manually, click the Server, and then click the **Disconnect**icon , or simply close the administration interface. (No confirmation message appears.)

IMPORTANT: If you click **File > Stop Server Service**, you will stop the EFT service and no clients will be able to connect to EFT.

Starting and Stopping EFT

EFT starts automatically and runs as a Windows system service. If you close the administration interface, EFT continues to run in the background as a system service.

On the Recovery tab of the service's properties:

- On non-HA installations, the service is configured to "Take no action" on failure.
- On HA installations, the service is configured to "Restart the Service" on failure.

For the procedure for a remote EFT connection, refer to Starting and Stopping EFT Remotely.

When you stop the service, EFT breaks all existing connections and waits until all socket threads die. The service can terminate when Timer Event processing is still in progress. The triggering of Monitor Folder and Timer Event Rules occurs almost simultaneously and is controlled by the operating system, not by EFT. Refer to Event Rule Order of Execution for more information.

To stop EFT in the administration interface

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server that you want to start/stop.
3. In the right pane, click the **General**tab.
4. Click **Stop service**, then click **Apply**. EFT status indicator turns from green to red.

To start or stop EFT using Windows Services

1. Click **Start > Run**. The **Run** dialog box appears.
2. In the **Open**box, type `services.msc`then press ENTER.
3. Right-click the **EFT Server** service and click **Start** (or **Stop**).

To start or stop EFT from the command line

1. Click **Start > Run**. The **Run** dialog box appears.
2. In the **Open**box, type `cmd`or `command`then press ENTER. The Windows **Command Prompt** dialog box appears.
3. To start EFT, at the prompt type the following command (include the quotation marks):

```
Net start "globalscape EFT"
```

4. To stop EFT, at the prompt type the following command (include the quotation marks):

   ```
   Net stop "globalscape EFT"
   ```

5. After the service is started or stopped, type **Exit** (or close the Command Prompt).

Secure the Server Service

Any time you run a service, you expose your computer to outside users. The potential exists for exposing files and programs on your computer and network to malicious outside users, particularly if EFT is compromised. Although you can set folder permissions from within EFT administration interface, you can add an extra level of protection by establishing a user account for EFT and then limiting folder access through EFT's user account permissions. This establishes a stopgap until server and system integrity can be restored if EFT is ever compromised.

To configure EFT to run securely, you should:

1. Create a user account for EFT
2. Assign permissions to EFT's user account and assign EFT to the account
3. Log EFT on as a service
4. If necessary, configure EFT's user account to map a virtual folder to a network drive.

Command-Line Login

After EFT is configured, you can open the administration interface and login automatically using the EFT computer's local administrator credentials from a command line or a Windows shortcut, using the EFT administrator listening IP address and port.

The EFT administrator listening IP address must be set to a specific IP address, not **All Incoming**. To log in remotely, remote administration must be configured and EFT must be in the same domain as the computer from which you are attempting to log in.

To open the EFT administration interface and login automatically at a command line

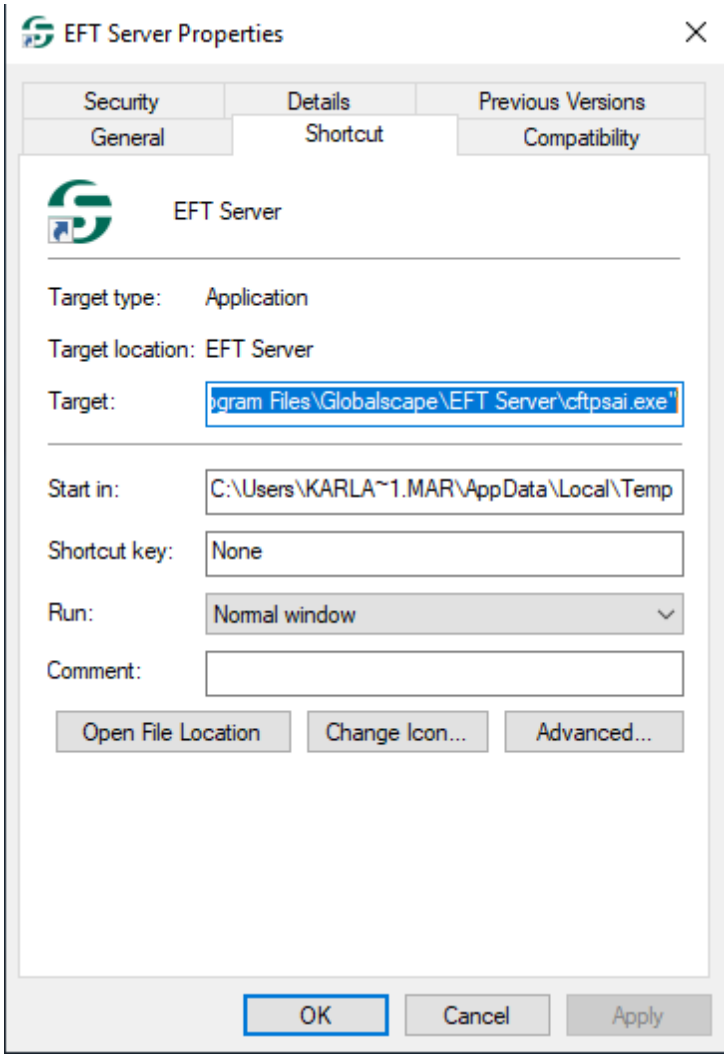
1. Open a command prompt (**Start > Run > cmd**).
2. Change to the directory in which EFT is installed (for example, **cd C:\Program Files\Globalscape\EFT Server**).
3. Type the name of the administration interface executable (**cftpsai.exe**), followed by the administrator listening IP address and port, then press ENTER. The IP address and port must be separated by a colon. For example, type:

   ```
   cftpsai.exe 192.168.174.142:1100
   ```

   The administration interface appears and logs in using the EFT computer's login credentials.

To open the EFT administration interface and login automatically using a shortcut

1. Right-click the EFT administration interface shortcut created when you installed EFT (or create one), then click **Properties**. The **Properties** dialog box appears.



2. In the **Target** box, after the quotation mark, add the administrator listening IP address and port. For example, the **Target** box would contain:

   ```
   "C:\Program Files\Globalscape\EFT Server\cftpsai.exe"
   192.168.174.142:1100
   ```

3. Click **OK** to save the changes.
4. Double-click the shortcut to test it. The EFT administration interface opens and logs in using the EFT computer's local administrator credentials.

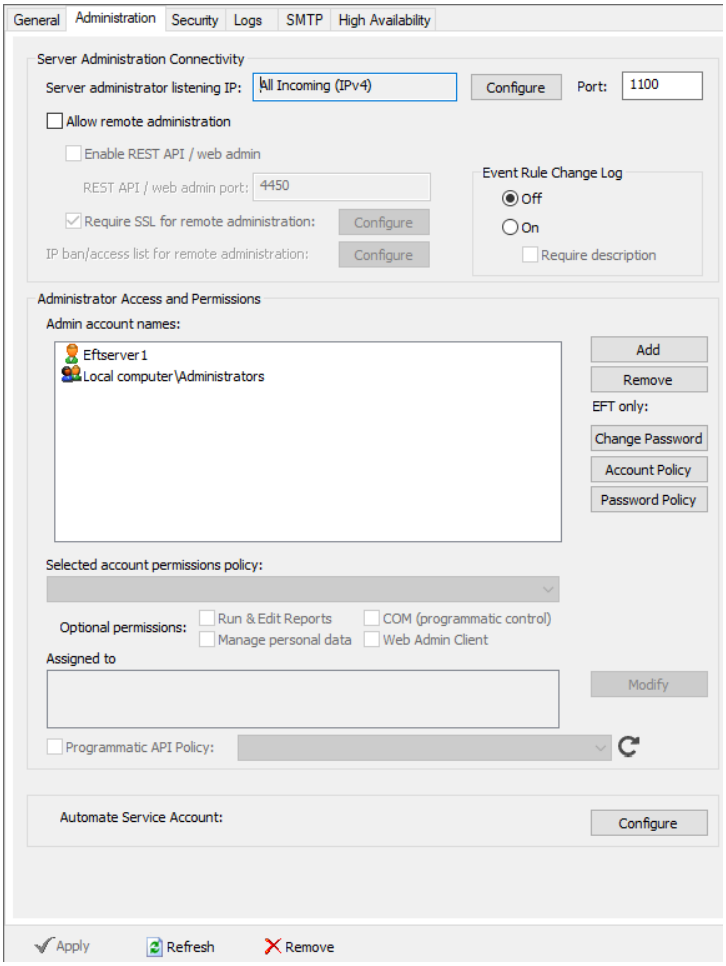
Listening IP Address and Port

EFT's administration listening IP address and port are configured in the EFT Server Setupwizard. You can change the IP address and/or port later, if necessary. For example, you might have initially configured EFT to listen on **All incoming** IP addresses and want to change it to a specific IP address, or maybe you need to add IPv6 addresses.

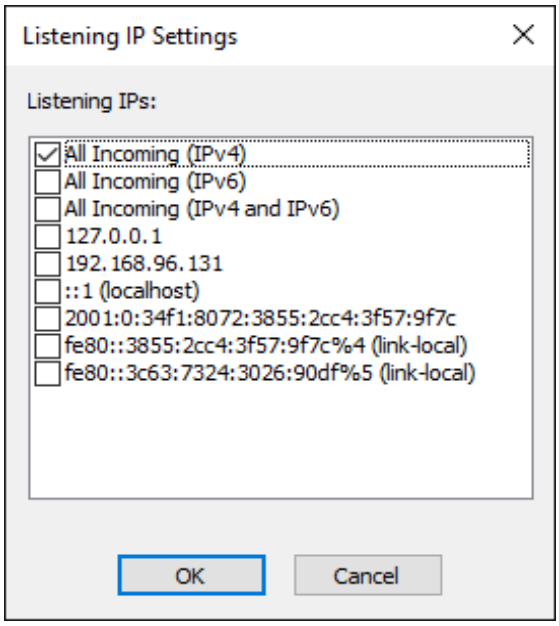
IPv6 addresses are not supported by MSMQ; however, a server and/or site can bind to IPv6, provided that there is also an IPv4 address (for example, another adapter) that can route between HA nodes.

To change EFT's listening IP address and port

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node that you want to manage.
3. In the right pane, click the **Administration**tab.



4. You cannot type an address in the **Server administrator listening IP** box. Click **Configure**. The **Listening IP Settings**dialog box appears.



   - The dialog box displays the IP addresses that are available on the computer, in addition to **All Incoming (IPv4)**and **All Incoming (IPv6)**.
   - IPv6 is not enabled by default for security reasons; IPv4 is enabled by default.
   - The "All" options are exclusive. That is, you can't select **All Incoming (IPv4)** and then one or more specific IP addresses. However, you can select multiple individual addresses if none of the "All" options is selected.
   - "Link local" appears next to certain IPv6 addresses. Routers do not forward packets with link-local addresses. In IPv6, link-local addresses are always assigned, automatically or by configuration, and are required for the internal functioning of various protocol components. IPv6 requires operating systems to assign link-local addresses to network interfaces even when routable addresses are also assigned. A link-local unicast address has the prefix fe80::/10 in standard IPv6 CIDR notation.

5. Select one or more check boxes for the IP addresses on which the Server is to listen for connections, and then click **OK**. The selected addresses appear in the **Listening IP addresses** box.
   - You can copy the addresses in the **Server administrator listening IP** box: Right-click in the box, click **Select All**, then right-click again and click **Copy**

or use CTRL+V. (Unicode-related items on the right-click menu are a Windows feature and do not apply to EFT.)

6. In the **Port** box, type the new port number.
7. Click **Apply** to save the changes on EFT.

Specify the Default Time Stamp

You can specify the default time stamp for directory listings to be the local Server time or UTC (Coordinated Universal Time)/GMT (Greenwich Mean Time) for FTP/S and HTTP/S.

SFTP listings and file dates always use UTC/GMT, even when the server is configured to use local server time.

If the time zone of the EFT computer is changed, you must restart the EFT service.

To specify the default time stamp

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Server that you want to manage.
3. In the right pane, click the **General** tab.
4. In the **Directory listing date stamp settings** area, click one of the following:
    - **Use local server time**
    - **Use UTC/GMT time**
5. Click **Apply** to save the changes on EFT.

This option is ignored when returning the “creation time” and “modification time” SFTP file attributes. SFTP file attribute messages always use UTC/GMT per the RFC, http://tools.ietf.org/id/draft-ietf-secsh-filexfer-13.txt. The FTP MDTM command always returns its results in UTC/GMT, independent of EFT's "Directory listing date stamp setting," per the associated RFC.

Deregister Licenses

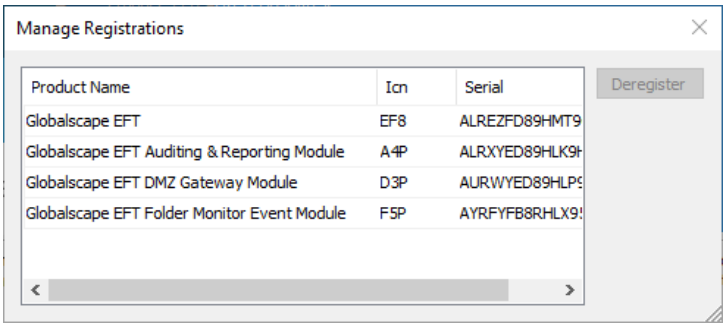
There are a variety of reasons why you might want to "deregister" the server and/or modules licenses, such as:

- You want to move EFT to a new computer
- You accidentally registered the wrong serial number
- A module was registered on the wrong server or node
- You are moving from a perpetual license to a subscription or from a subscription to perpetual.

Deregistering the license on one server will allow you to reactivate the license on a another server.

To deregister a license

1. Open the EFT administration interface, then on the main menu, click **Help > About EFT**.
2. In the **About EFT Server** dialog box, click **Manage**. The **Manage Registrations** dialog box appears.



3. Click the product that you want to deregister, then click **Deregister**.

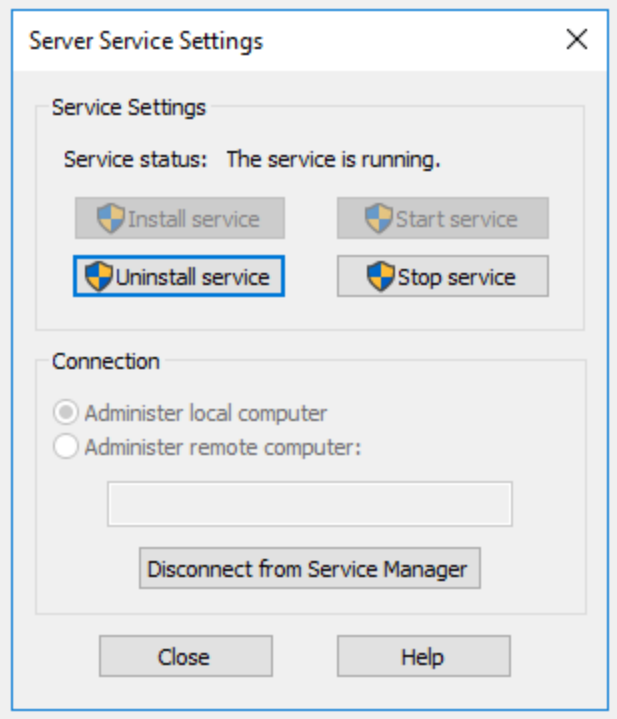
The dialog box refreshes and the selected product is removed from the list. The license is now available to register on another server.

Administering the Server Service

The **Server Service Settings** dialog box is used to administer the EFT server service, either locally or remotely. Using this dialog box, you can uninstall/install the service and stop/start the service instead of opening the Services Microsoft Management Console (MMC) snap-in.

To administer the EFT service

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the main menu, click **Edit > Server Service Settings**. The **Server Service Settings** dialog box appears.



- To stop the service, click **Stop service**. (You can also stop the service on EFT's **General** tab.)
- To start the service, click **Start service**.
- To remove the service, click **Uninstall service**. (The application is not removed from the computer, it's just not accessible in Windows.)
- To reinstall the service and make it accessible from Windows, click **Install service**.
- To administer a remote computer

a. Click **Disconnect from Service Manager** to make the **Connection** area available.
b. Click **administer remote computer**, then type the IP address of the remote computer, including the port if different from the default. For example, type `192.168.20.47:1101`.

- To administer the local computer (if remote was previously selected)
  a. Click **Disconnect from Service Manager** to make the **Connection** area available.
  b. Click **administer local computer**, and then click **Close**.

Related Topics

- Logging In to administer EFT
- Starting and Stopping EFT
- Starting and Stopping EFT Remotely

Advanced Properties

"Advanced Properties" are settings used when the administrator wants to enable, disable, or "set" certain properties used by EFT that are different than the default settings. For example, you might want to set a longer or shorter period for HTTPS socket timeout, or specify different logging options. You do this by adding the name of the property and a non-default setting to the **AdvancedProperties.json**in EFT's \ProgramData\ directory.

When you upgrade from 7.4.x to 8.x, the registry settings in the previous version that are **not** using the default settings are copied to **AdvancedProperties.json**and then deleted from the registry.

Refer to the Advanced Properties PDF for a list of advanced properties.

What is a JSON file?

JSON is an open-standard file format similar to XML that is human-readable and easy to edit. The JSON file contains name/value pairs or objects surrounded by " (double quotation marks). An object begins with **{** (left curly brace) and ends with **}** (right curly brace). Each name is followed by **:** (colon) and the value: "name": value or "name": "value".

For multiple advanced properties, add a comma after each name/value pair, except the last one.

(See an example in the procedure below. Refer to https://tools.ietf.org/html/rfc8259#section-3for more information about JSON files.)

How does the AdvancedProperties.json work in EFT?

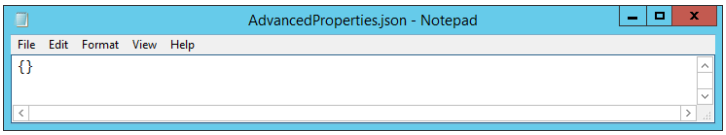
- **AdvancedProperties.json** *is created for you*in the **ProgramData** folder for EFT (for example, **C:\ProgramData\Globalscape\EFT Server**) after the EFT server service is started. You do ***not*** have to create the file. If you change the file name, introduce a typo, or created a duplicate file with a different name, EFT will ignore it.
- EFT reads **AdvancedProperties.json** anytime the EFT server service is started.
- If you don't see the **ProgramData**folder, in Windows File Explorer, click **View**, then select the check box next to **Hidden items**. You could also select the check box for **File name extensions** to see the JSON extension.

How do I change or add advanced properties?

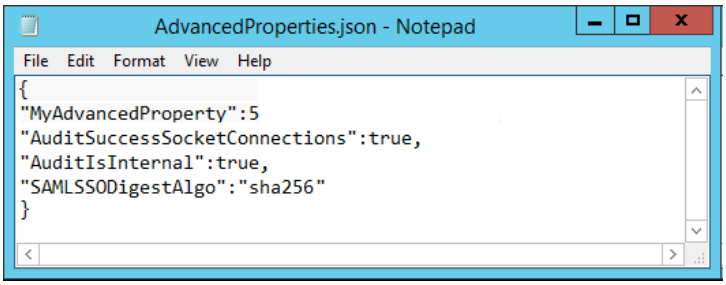
- Before you start editing this file (if it is **not**blank, meaning you have non-default settings defined), please make a backup copy with a different name in case you need to roll it back.
- A JSON value MUST be an object, array, number, string, or one of the following three literal names: **false**, **null**, or **true**. (The literal names must be lowercase. No other literal names are allowed.)
- JSON file entries are **case sensitive**. You must enter the format as expected, otherwise the EFT service will fail to start. That is, if EFT was expecting "EncryptPersonalData" but you spelled it "EncryptPersonelData" EFT will ignore it.
- EFT doesn't validate the JSON file itself for acceptable or unacceptable names and values. It only reads names and validates their values. If the "value" is wrong or malformed, the EFT server service will not start, and an error is written to the log.
- If the Advanced Property name is misspelled, it is ignored, but the service will start.

To edit or view the Advanced Properties file

1. Navigate to the EFT installation folder, then open **AdvancedProperties.json**in a text editor (such as Notepad). In a new installation of EFT, or in an upgrade with only default EFT-related registry settings defined, the file will be blank, except for two curly brackets: `{ }`



   If you are upgrading from a prior version with ***non-***default registry settings, EFT will import them during upgrade and you will see them in the JSON file.



2. To add a new name/value pair:

a. Add a new line after the opening bracket.
b. Type the name of the object, with the name surrounded by double quotation marks, followed by a colon (:), then a space, then the value.
   - Strings must be enclosed in quotation marks.
   - Numbers and literal names (false, null, or true) do not need quotation marks. (Shown in screenshot above.)
c. For multiple objects, add a comma after the value, then add a new line and type the second object.(Do not add a comma after the last value before the closing bracket.
d. Add a new line after the name/value pair, before the closing bracket.

3. Save the file.
4. Stop and restart the EFT server service, and then refresh the user database (**View > Refresh User Database**).

FAQ

1. **If I have (for example) 100 EFT-related registry settings in EFT v7.4.13, then upgrade to v8.x, do my EFT registry settings become ineffective?**
   No. The existing registry settings that are ***non-default***values are migrated to the JSON file and then deleted from the registry. EFT will still read the registry, but it's recommend that you only add new items to the JSON file instead of the registry.
2. **Do I have to recreate/reenable each of my EFT registry settings in the JSON file?**
   Upon upgrade to EFT v8.x, any EFT registry entry that is configured as a ***non-default*** value will be migrated to the JSON file. Anything that is configured with a default value (the equivalent of it not being enabled) will be ignored and not added to the JSON file.
3. **Do I have to remove the old registry settings?**
   Upon upgrade from 7.4.x to EFT v8.x, any registry entry that is migrated to the JSON file will be removed from the registry.
4. **Are the advanced properties logged in EFT.log?**
   Only **non-default** advanced properties are logged.
5. **Is JSON file backup/restore supported?**
   Yes.
6. **If I add an Advanced Property to the JSON file that is default behavior, will that prevent EFT service start?**
   No, it does not prevent EFT service start. The EFT service will start if the format is correct; however default values will not show up in the EFT.log on service start.

Topics that Reference Advanced Properties

- Personal Data Encryption
- GDPR Settings
- Specifying a User Disk Quota
- Login to EFT (WTC)
- Display Full Name of User in WTC on LDAP Site
- Starting or Stopping a Site
- SFTP FIPS
- Configuring SFTP for a Site
- Specifying the Value Returned by the FTP SYST Command
- OCSP
- Redirecting HTTP to HTTPS
- Enabling DMZ Gateway in EFT
- Encrypted Folders (EFT built-in, Secure-Data-at-Rest Solution)
- Copy/Move Download File Cloud Storage Actions
- Backup Server Configuration Action
- Event Rules Client Log
- EFT.log File
- Event Rule Load Balancing
- Backing Up or Restoring Server Configuration
- Unicast
- EFT Specifications
- SSO Process
- AD Password Expiration
- Installing and Configuring the Auditing and Reporting Module
- EFT Database Utility

Email Server Settings

The **SMTP Server Settings** on EFT's **SMTP** tab are completed automatically when you define them in the **Server Setup Wizard** during installation. You must configure the mail server settings for the EFT to send email notifications when Eventsoccur, including the address for the outgoing mail server, an address for the administrator, and other details described below.**Email Templates** used for notifications are also managed at the bottom of the **SMTP** tab, and saved in the SQLite database found in **..\ProgramData\Globalscape\EFT Server**.

Microsoft recommends that you disable SMTP AUTH organization-wide or per mailbox (hosted in Office 365 or Microsoft 365). For more details, refer to the Microsoft topic at https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission.)

In EFT v8.2 and later, SMTP can authenticate with the XOAuth2 method. XOAuth2 can be configured from the EFT administration interface, REST API, and COM API. The supported token providers are Gmail or Microsoft 365. Google provides Gmail service account credentials in a key file. An EFT administrator needs to specify a path to the key file (which works similar to EFT SSL certificates).

NOTE:

- SMTP does not support Unicode characters. Refer to Unicode Exceptions for details.
- The SMTP server settings in EFT should be propagated to the Advanced Workflow module for use in Email actions.
- If you want to change or verify these settings in the AW module, refer to Knowledgebase article at https://kb.globalscape.com/KnowledgebaseArticle11423.aspx.
- Also refer to the Automate Desktop help regarding Email options.

Related Topics

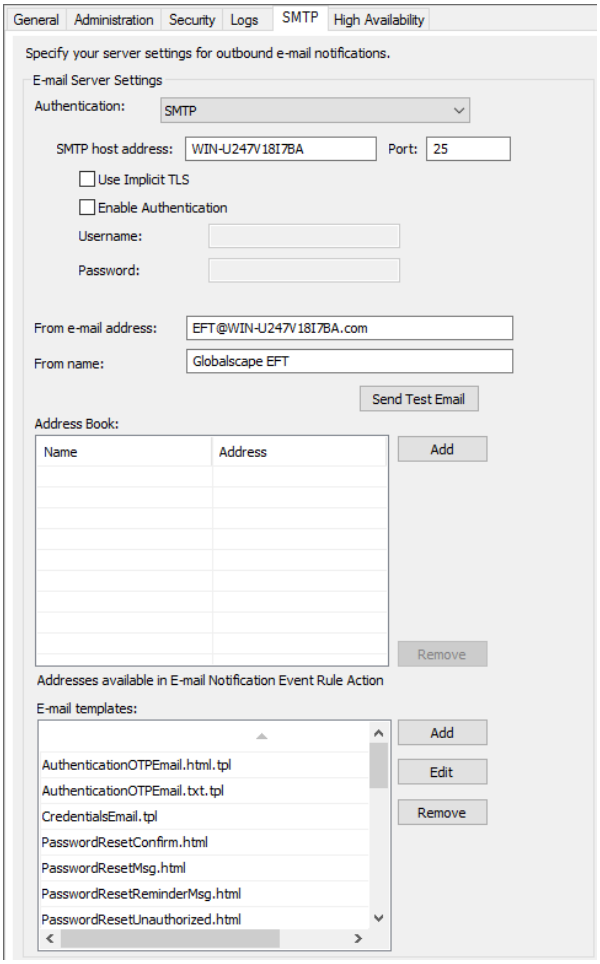
- Configuring Email Server Settings
- Create a New Secret for OAuth
- Create Admin Account for OAuth - Microsoft 365
- Create a Gmail Service Account

Configuring Email Server Settings

The **Email Server Settings** area on EFT's **SMTP** tab are completed automatically when you define them in the **Server Setup Wizard** during installation. You must configure the mail server settings for the EFT to send email notifications when Eventsoccur, including the address for the outgoing mail server, an address for the administrator, and other details described below.

To configure EFT to send email notifications

1. Click the **Server**tab in the administration interface and select the Server that you want to configure.
2. In the right pane, click the **SMTP**tab.
3. Under **Email Server Settings**, in the **Authentication** drop-down list, select the email server type to which you want to connect: **SMTP**, **Gmail OAuth**, or **Microsoft 365 OAuth**.

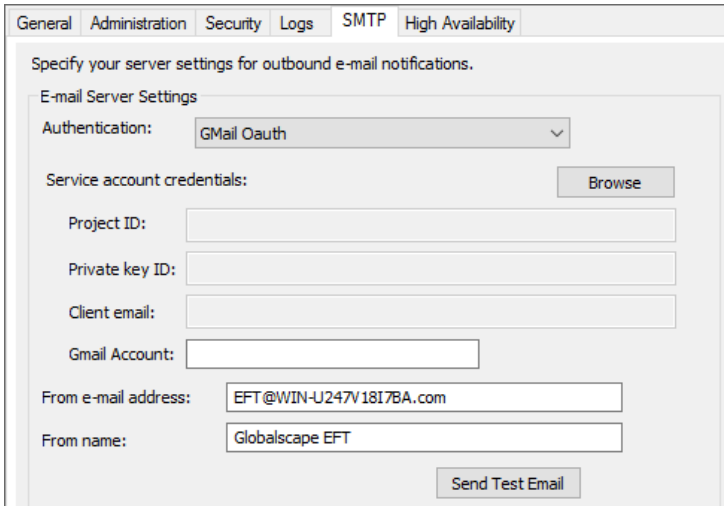


For SMTP

- In the **SMTP host address** box, specify the address of the mail server EFT will use to send outgoing messages. (If you have any trailing spaces in the host address, the address will not resolve. Be sure if you are copying and pasting an address into the dialog box that you are not including any spaces.)
- In the **Port**box, specify the port number at which the mail server accepts messages. The standard is **25**.
- Select the **Use Implicit TLS** check box, if required by your SMTP server.
- Click the **Enable Authentication** check box if the SMTP server requires that EFT login to connect, then provide the **Username**and **Password**.

For Gmail OAuth

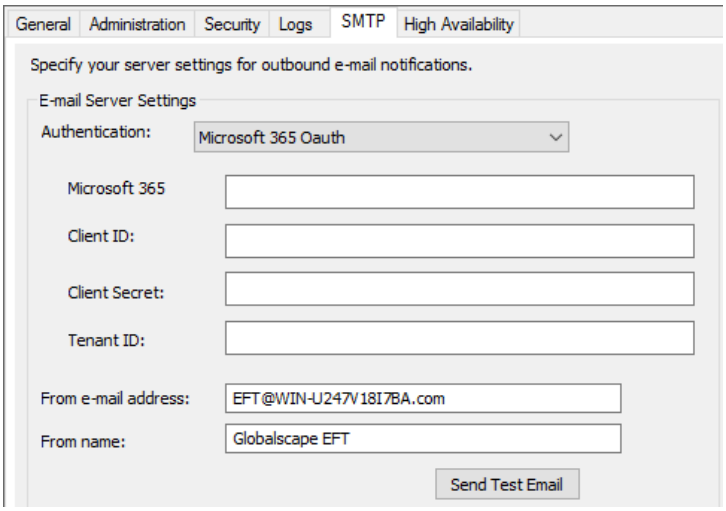
> **NOTE:** For details of creating the Gmail service account credentials and JSON file, refer to Create a Gmail Service Account.



- In **Service account credentials**, click **Browse** and select the file that contains the **Service account key json path** file. The fields will be completed with the information from the JSON file.

For Microsoft 365 OAuth

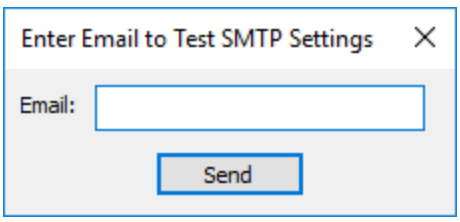
For details of using Microsoft 365 OAuth, refer to Create a new Secret for OAuth and Create Admin Accoutn for OAuth - Microsoft 365.



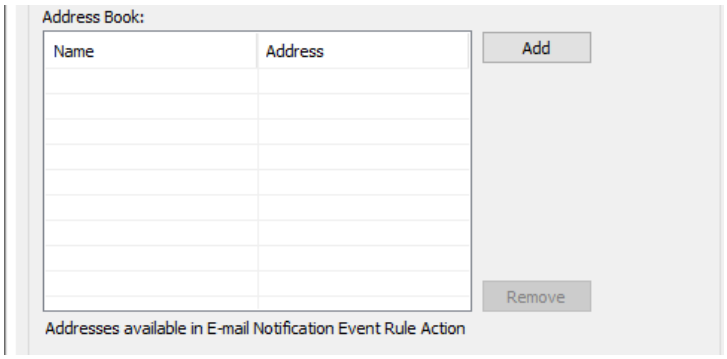
- **Complete the fields to connect to the Microsoft 365 mail server:**
  - Microsoft 365 - Email address used when you created the Client Secret.
  - Client ID - The application (client) ID that's assigned to your app.
  - Client Secret - Refer to Create Admin Account for OAuth -Office 365. If you did not record the secret when you created it, refer to Create a New Secret for OAuth.
  - Tenent ID - The directory tenant the application plans to operate against, in GUID or domain-name format.

> **NOTE:** Microsoft recommends that you disable SMTP AUTH organization-wide or per mailbox (hosted Microsoft 365). For more details, refer to the Microsoft topic at https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission.)

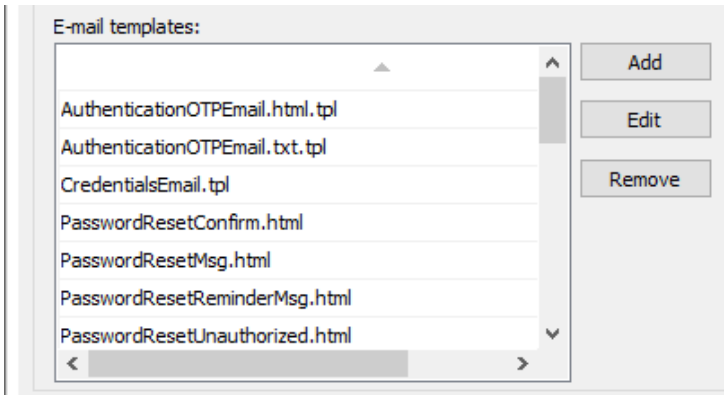
4. Provide the **From email address** and the **From name** that will appear in email notifications *sent from EFT*. An error message appears if the email address is not properly formatted.
5. To verify your SMTP configuration, click **Send Test Email**. The **Enter Email** dialog box appears.



6. Enter an email address to send a test email to, then click **Send**. A confirmation message appears.
7. Click **OK**to dismiss the message. The **Send Test Email** button sends the email directly (synchronously). If you receive the test email, the SMTP configuration is correct.
8. In the **Address Book** area, click **Add** to add names and email addresses of recipients of EFT Event notifications. Add only the addresses that you want to receive email notifications. The email addresses will be added automatically to the **To**box in the Send notification email Action in Event Rules.

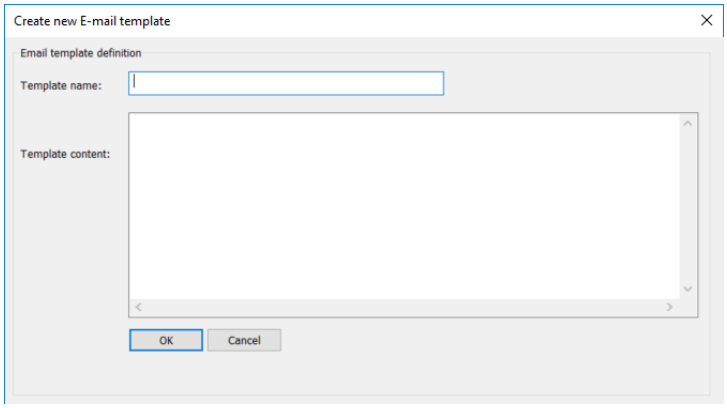


   - To edit a name or address, click once to select the box, and then click again to activate the box.
   - The email addresses added to the Address Book are validated for format when you click **OK**. If the email address contains invalid characters or does not contain @, an error message appears. Click **OK**to dismiss the error message, then correct the address.
   - To remove an email address, select the address, then click **Remove**.
9. In the **Email templates** area, you can add, edit, and remove email templates used by EFT and Workspaces to send notifications regarding authentication, credentials, passwords, and PGP key expiration errors. (Refer to EFT Messages and Templates for details of the templates.)



To add a template

a. Click **Add**. The **Create New Email Template** dialog box appears.



b. Provide a **Template name**, then add the **Template content**. You can create an HTML version with HTML tags (<html> <body> <p> and so on) and variables, such as %USER.FULLNAME%, or a TXT version without the HTML tags, and using variables.

c. Click **OK**.

To edit a template

a. On the **Server > SMTP** tab, in the **Email Templates** area, click to select a template, then click **Edit**. The **Edit Email Template** dialog box appears.

b. The **Template name** cannot be edited.

c. In the **Template content** area, make your edits, then click **OK**.

To remove a template

- On the **Server > SMTP** tab, in the **Email Templates** area, click **Remove**. A message appears saying that the selected template will be removed. (There is no "undo.")

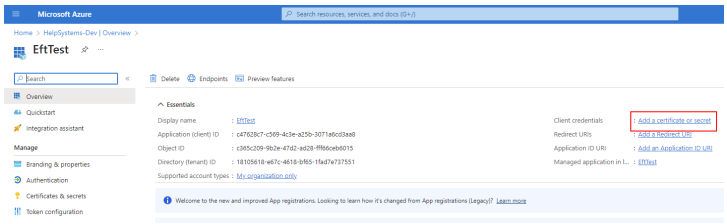
10. Click **Apply**to save the settings on EFT.

Create a New Secret for OAuth

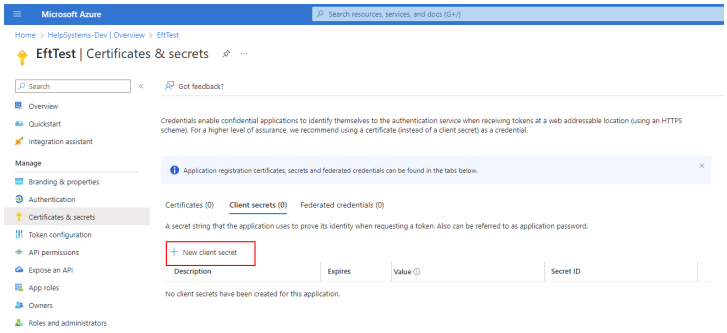
When OAuth (GOOGLE, OUTLOOK) is selected for authentication and emails are not being received, you may need to create a new secret for OAuth.

To create a new secret for OAuth

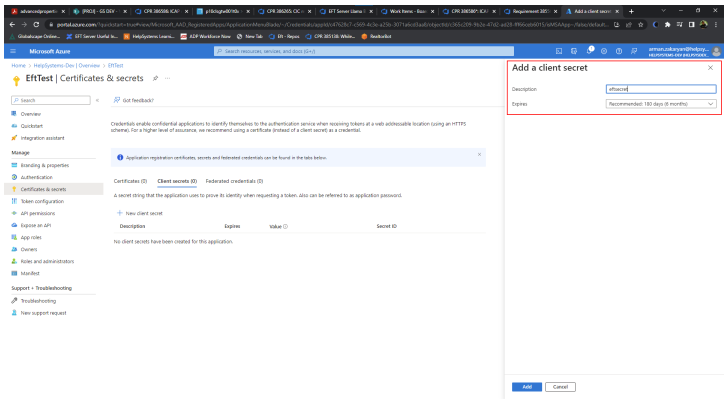
1. Log into the Azure account
2. In the **Overview** tab, then click **Add a certificate or secret**.



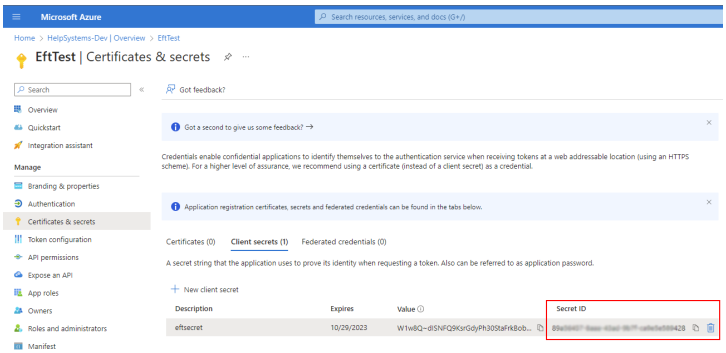
3. Click **New client secret**.



4. Give the secret a name



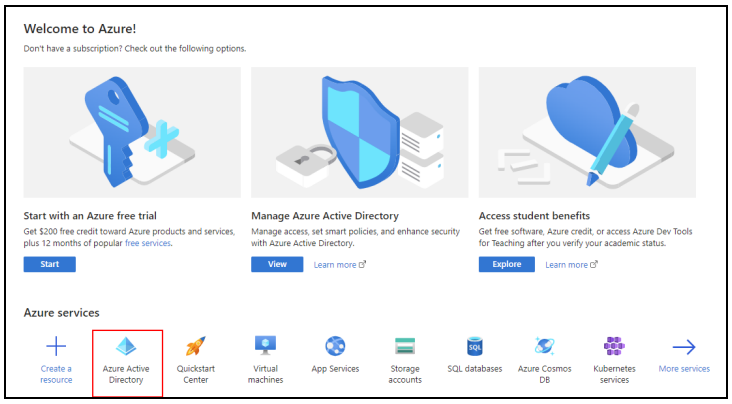
5. Save the secret value, as it will not be accessible later.



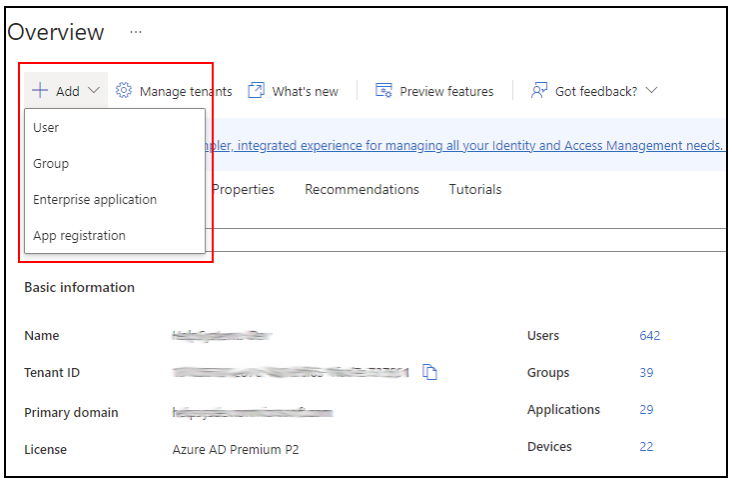
Create Admin Account for OAuth - Microsoft 365

To enable OAuth for Microsoft 365

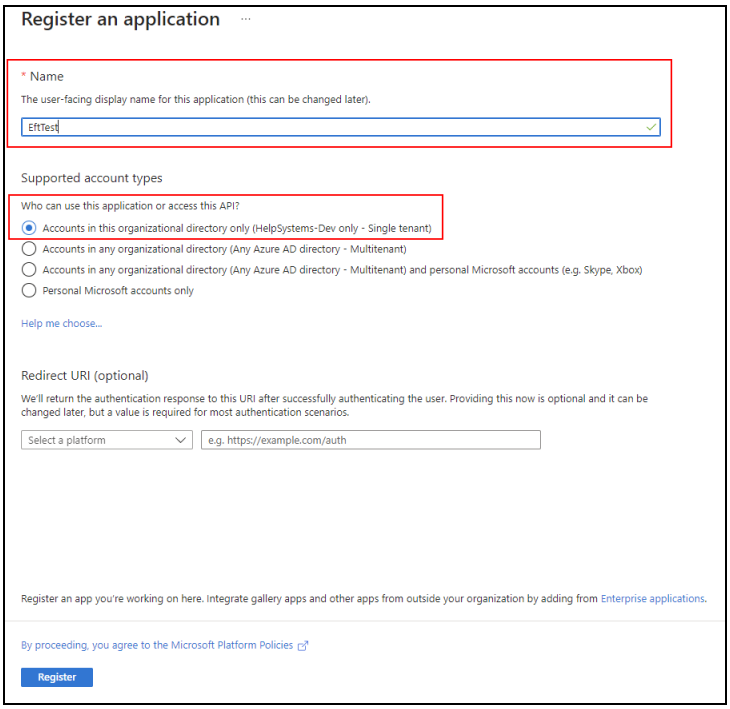
1. Create an administrator account in Azure, such as `admin@eftserverlocal.com`.
2. In portal.azure.com, click the **Azure Active Directory** icon.



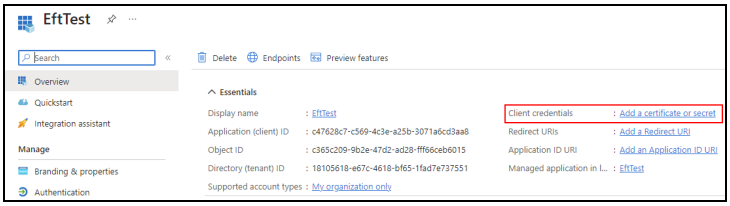
3. The **Overview** page appears. Click the **Add** drop-down, and then click **App registration**.



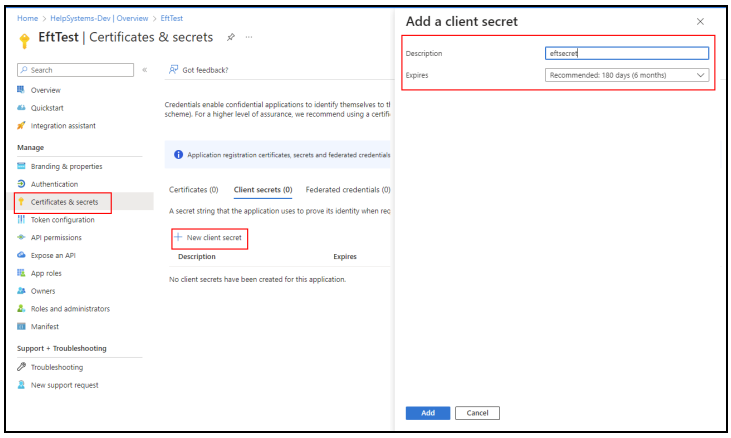
4. The **Register an application** page appears.



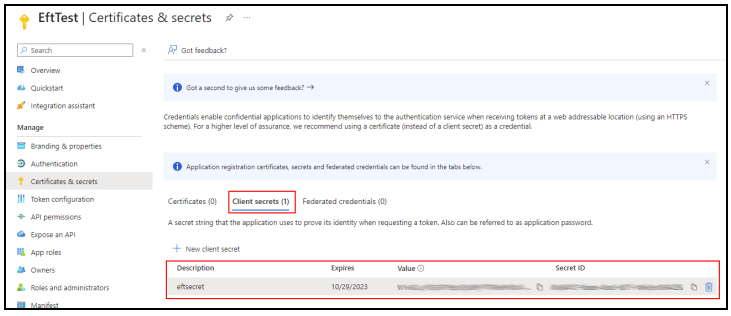
5. Provide a unique, user-facing name for the application, such as EFT. (You can change it later.)
6. Under **Supported account types**, keep the default of **this organizational directory only**. Then click **Register**.
7. On the application page (in this case, EftTest), next to Client credentials, click **Add a certificate or secret**.



8. The **Certificates & secrets** page appears. Click **New client secret**. The **Add a client secret** section appears.
9. In the **Description** box, type a name for this secret.

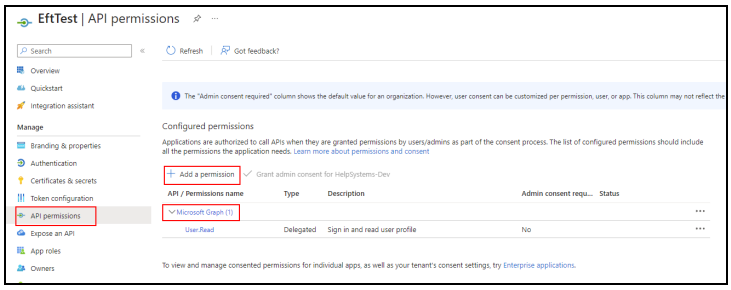


10. The secret appears under the **Description** on the **Client secrets** tab.



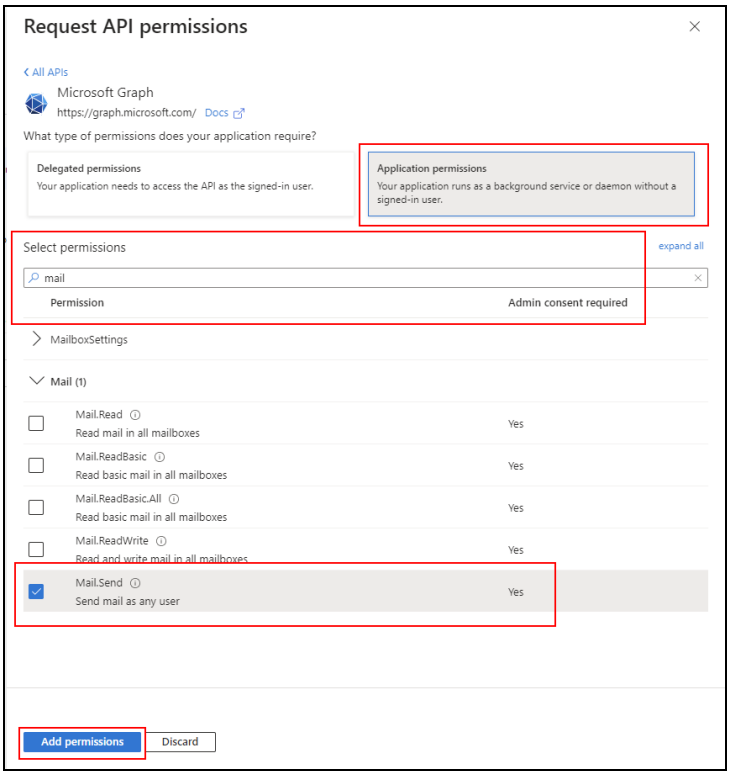
> **NOTE:** The application uses the secret string to prove its identity when requesting a token. It can also be referred to as the application password. **Save the secret value as it will not be accessible later.** You can use the copy icon to copy the secret and paste it into wherever you save such things.

11. Click **API permissions**. The **API permissions** page appears.

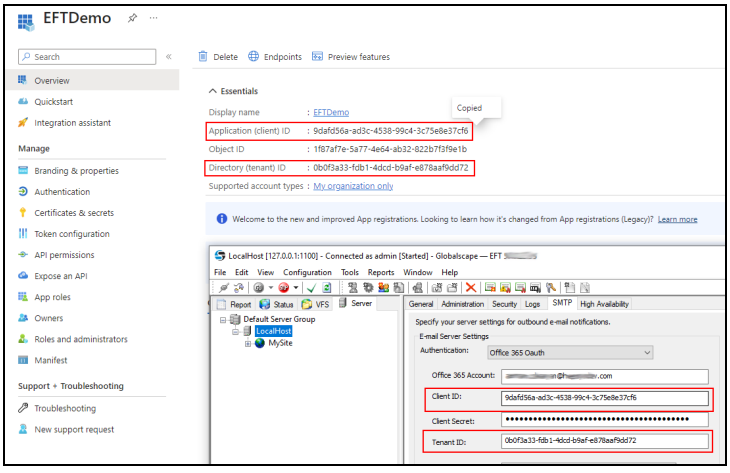


12. Click **Add a permission**, then click the **Microsoft Graph** drop-down. The **Request API permissions** section appears.

> **NOTE:** Microsoft Graph is a Microsoft API developer platform that connects multiple services and devices.



13. Click **Application permissions**, search for "mail," then click select "Mail.Send."
14. Click **Add permission** to close this window, then click **Grant admin consent** on the API permissions page.
15. Click **Overview**. Copy the data to the **Email Server Settings** in EFT on the **SMTP** tab.



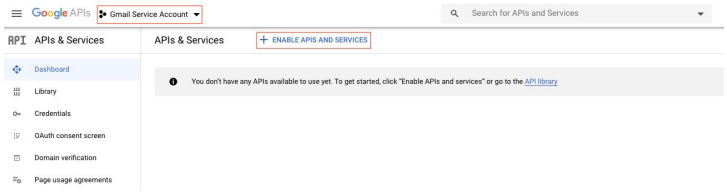
Create a Gmail/ Google Cloud Service Account

The procedure below describes how to create a Gmail service account in the Google Client Platform. A service account represents a Google Cloud service identity, such as Compute Engine VMs, App Engine apps, or systems running outside of Google. After you have created the service account, you can use the JSON file and your Google service account credentials in the **Server > SMTP** tab as described in Email Server Settings.

> **NOTE:** Your personal Gmail email account cannot be used as a Google Cloud Platform administrator. You will need to create a Google Workspace administrator account. You can read more about Google Workspace here https://workspace.google.com/faq/.

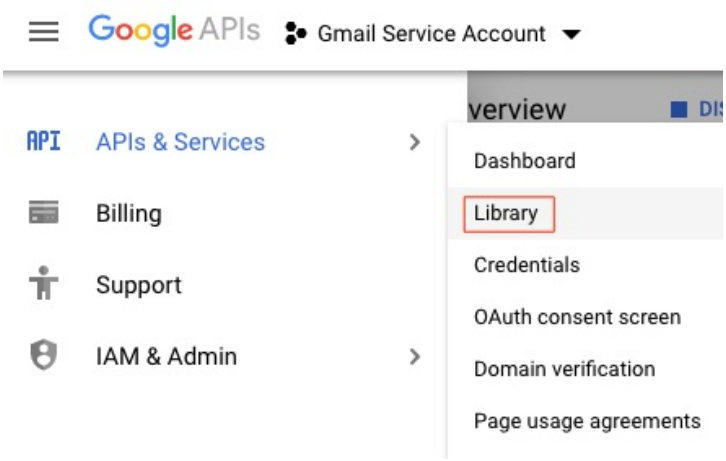
To create a Gmail service account

1. Navigate to Google Cloud Platform (GCP) console: https://console.cloud.google.com/.
2. Login with your Google administrator account.
3. To create a new project, click **APIS AND SERVICES**.

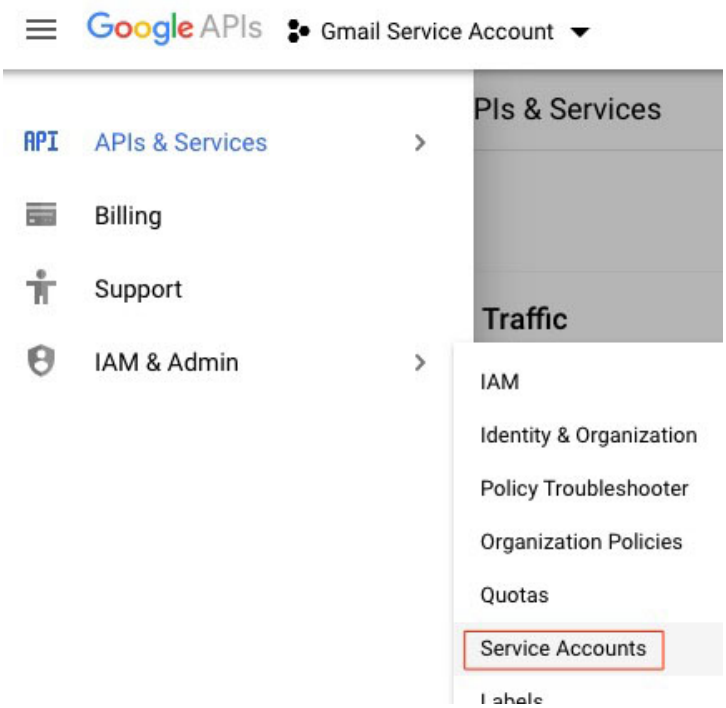


4. Click **+ ENABLEAPISANDSERVICES**.
5. In the API library, search for the following API sets. Click each set and then click Enable.
    a. Gmail API
    b. Google Calendar API
    c. Contacts API
    d. People API

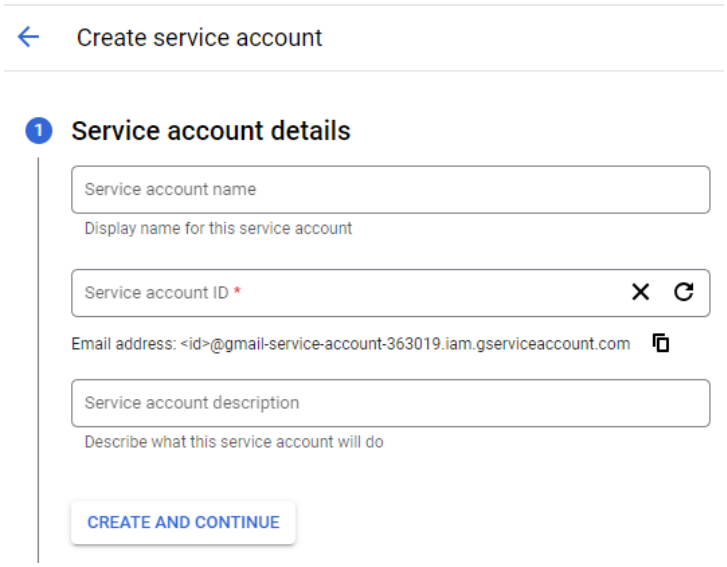
> **NOTE:** Navigate back to the API library by clicking the ☰ menu and then click **APIs & Services > Library**.



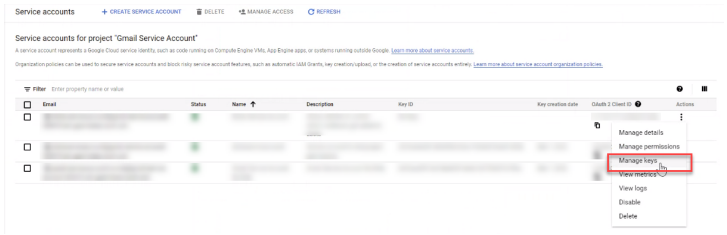
6. In the API & Services > Library, click **IAM & Admin > Service Accounts**.



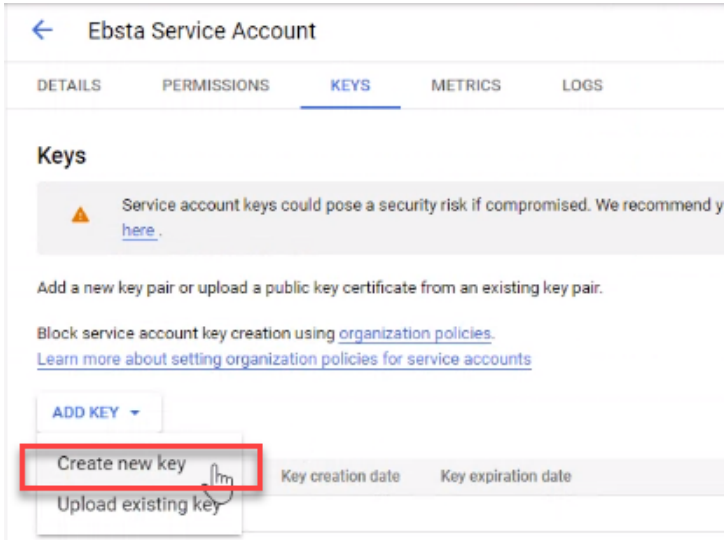
7. At the top of the **IAM & ADMIN** page, next to **Service accounts**, click **CREATE SERVICE ACCOUNT**.



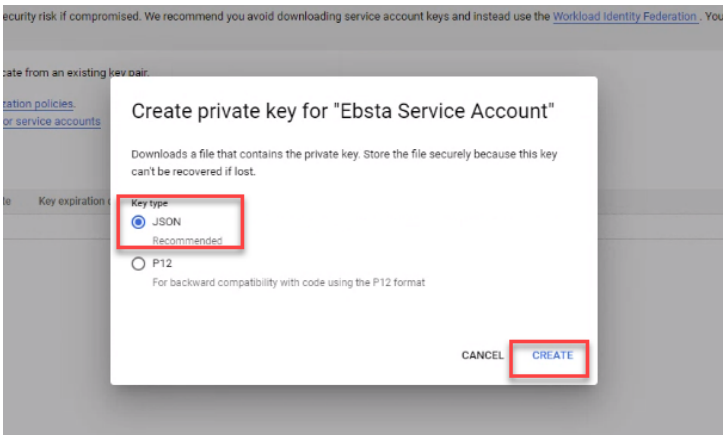
8. Fill in the details of the account and then click **CREATE AND CONTINUE**.
9. Click **Done**.



10. On the **Service accounts** page, under the **Actions** column, select the recently created service account then click **Manage keys**.



11. On the account page, click **Create new key**.



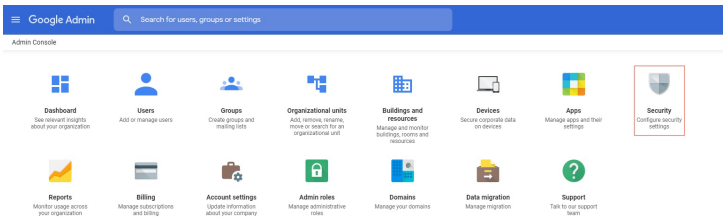
12. In the dialog box that appears, under **key type** click **JSON** then click **CREATE**.

> **NOTE:** Capture the Client ID* as this will be needed later!

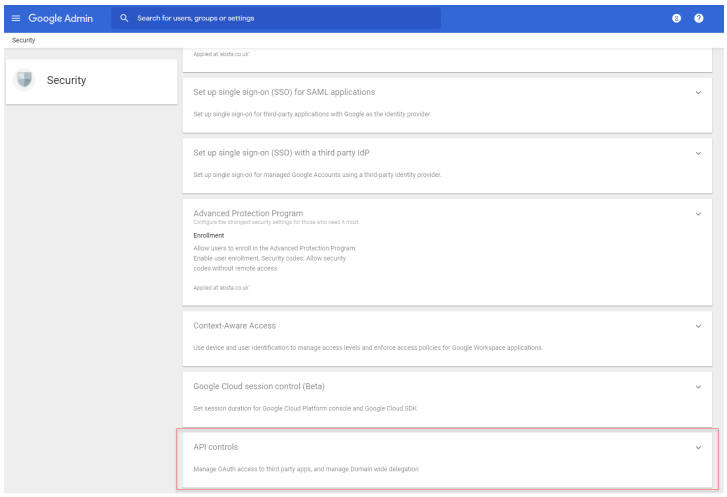
13. The JSON file should be downloaded to your computer. You must store this securely as it provides access to your resources. Click **Close**.

The next steps will enable the service account with Gmail.

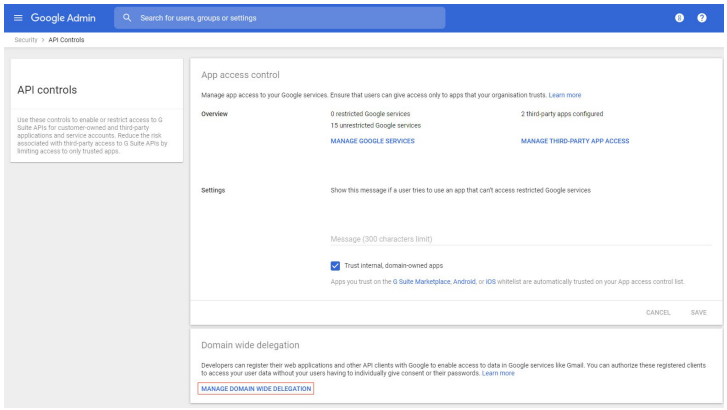
1. Login to the **Gsuite Admin Console**: https://admin.google.com, and then click the **Security** icon.



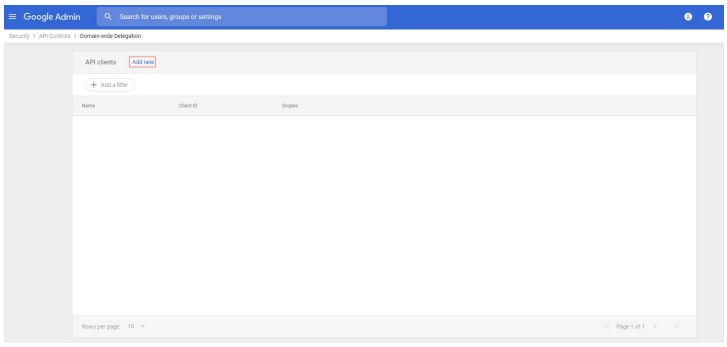
2. Under **Access and data control**, click **API controls**.



3. Click **Manage Domain Wide Delegation**.



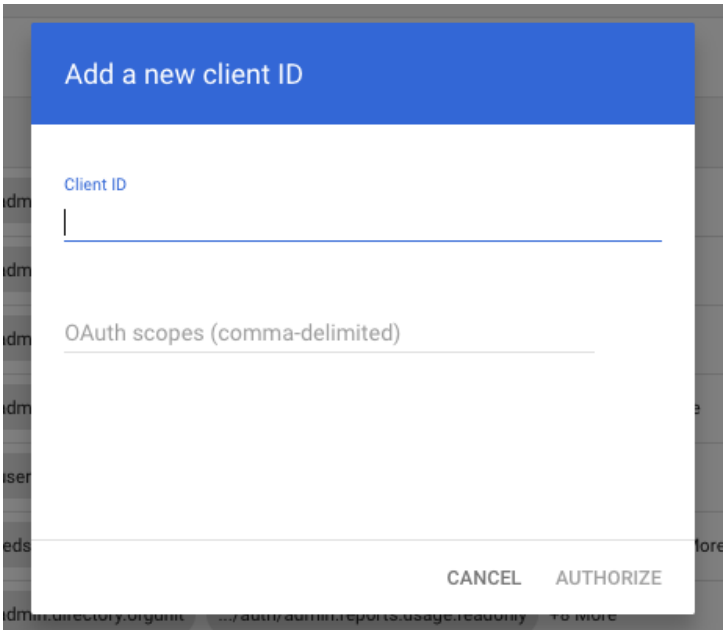
4. Click **Add New**.



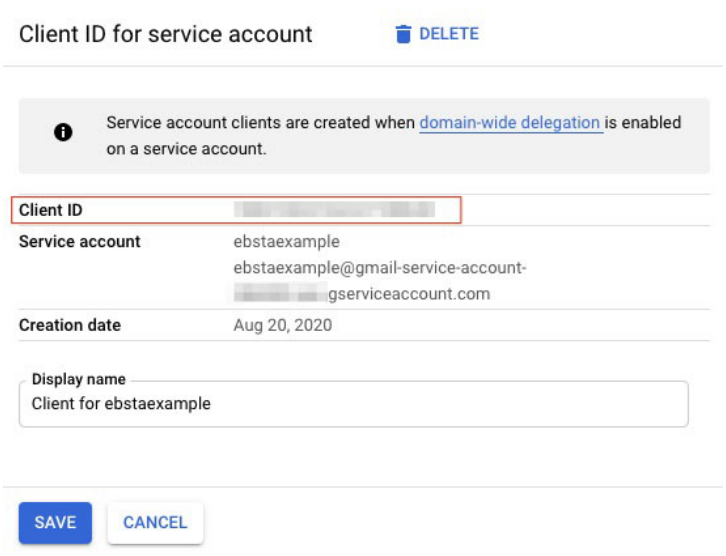
5. **Add the following scopes to the service account previously created:**
    - https://www.googleapis.com/auth/gmail.readonly
    - https://www.googleapis.com/auth/calendar

- https://www.googleapis.com/auth/gmail.send
- https://mail.google.com/

6. Provide the Client ID, and then click **Authorize**.



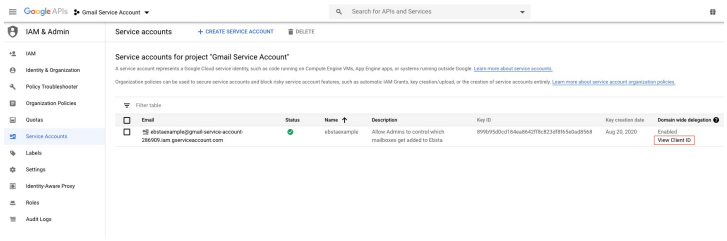
7. Enter the **Client ID** from the previous configuration. (Later, you can use the procedure below to find your Client ID).



8. Click **Save**.
9. Wait 5 minutes for the account to propagate correctly.

To find your Client ID

Client ID is the unique ID of the Service account client (not the Key ID). It can be found by clicking the ☰ menu in the GCP console and selecting **IAM & Admin > Service accounts**. Click **View Client ID** and then copy it onto your clipboard.



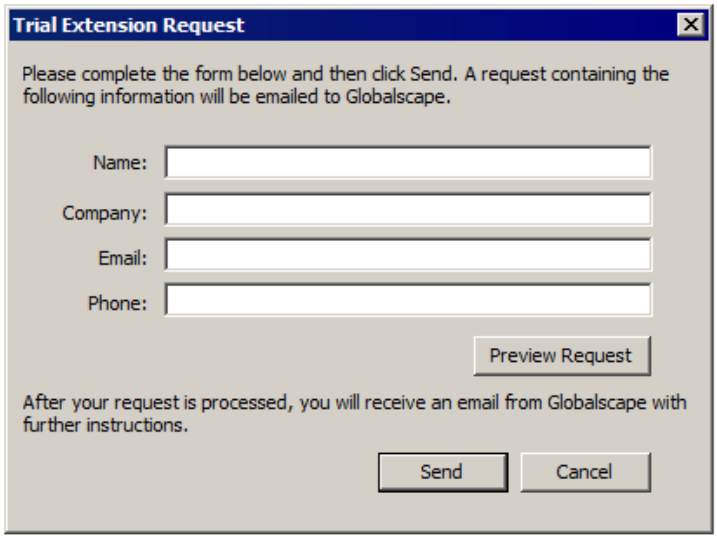
Extending the Trial

After trial expiration, EFT blocks all incoming client IP addresses. All outgoing (offload/download) requests from EFT's Event Rules are also blocked to any IP address. Therefore, when the trial period is over, no external IP addresses can connect to EFT, nor can EFT connect to any external IP addresses.

EFT has many complex features that you will want to take time to evaluate thoroughly. Therefore, the initial trial might not be enough time for busy IT professionals to make a buying decision. For this reason, you can request a trial extension that, if approved, provides time of full functionality, including add-on modules.

To request a trial extension

1. Open the administration interface.
2. On the main menu, click **Help > Request Trial Extension**. The **Trial Extension Request** dialog box appears.



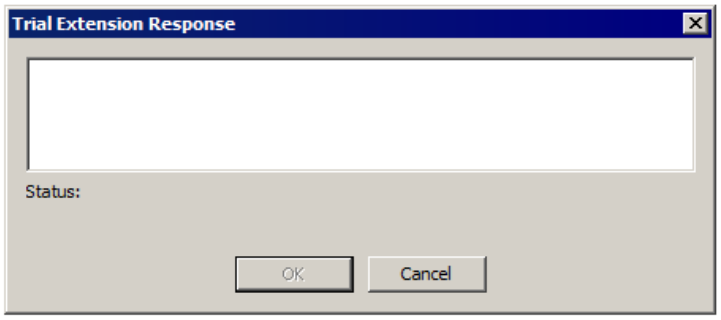
3. Provide your **Name**, **Company**, **Email**address, and **Phone**. This information is used to find your account in our database.
    a. If you would like to review the request before sending it, click **Preview Request**. The **Trial Extension Request Details**dialog box appears.
    b. Click **Close**to close the dialog box and return to the request.
4. Click **Send**. Your request is sent to the Globalscape server, which will forward your request to an account executive. If your computer does not have access to the Internet, copy the trial extension request to a computer that has internet access and email the request to your account representative, or if you don't

have one, use the Contact Sales form online at https://www.globalscape.com/support/contact-us. After your request is processed, an account executive will send you an email with a response string.

- If you do not have Internet access from the EFT administration interface, an error message appears. You can copy the contents of the Trial Extension Request to the clipboard and then email to Globalscape Sales using the form at https://www.globalscape.com/support/contact-us.

To provide the Trial Extension Response

1. Log in to the administration interface. (You must be logged in to EFT on the computer from which the trial request originated.)
2. On the main menu, click **Help > Enter Trial Extension Response**. The **Trial Extension Response** dialog box appears.



3. Copy the string from the email and then paste it into the **Trial Extension Response**dialog box.
   - If the string is not valid, an error message appears. Verify this is the same computer from which the trial extension request originated and that you have copied the exact response from the approval message.
   - If the string is validated, click **OK**.
4. If the string is accepted, the trial is extended.

Connection Problems

If you are having problems connecting to EFT, verify the following information:

- Your username and password are correct. Each is case sensitive.
- The Host (the IP address) and port are correct. Refer to Remote administration.
- The IP address from which you are trying to connect is allowed to access EFT.
- The EFT service is running. Refer to Starting and Stopping EFT.
- The network connection is functioning.

If the EFT service is not running, you may be able to start the service remotely.

When files are being transferred with Event Rules (copy, move, or download), if there are connection problems (for example, the network is unavailable), EFT will attempt to establish a connection the number of times specified in the Event Rule. When EFT is able to re-establish the connection, it continues to transfer the file from where it stopped, even if there are multiple interruptions. There are no retry attempts after a login failure.

If the network is lost while the Web Transfer Client is transferring files, it waits for a timeout period (30 seconds) and then shows a red X for the transfer. The **Status**in the queue pane indicates that the transfer failed. If you want to attempt to transfer the file again, you must login again when the network is available. After the Web Transfer Client reconnects, it resumes the transfer from where it stopped.

DNS-Rerouting

When EFT attempted to connect to a host, such as an AD server for user authentication or to refresh its user list, it could, occasionally, fail to connect due to network changes. EFT will attempt to bind to a host using the known Domain Controller (DC) for host values specified in EFT, as a server DNS, domain DNS, or Global Catalog. If it again fails to connect, EFT will update the DC, and then attempt to bind again; if it continues to fail, EFT will log the bind failure.

Specifying a New Local or Remote EFT

After you have configured the local connection to EFT (that is, a connection on the same computer on which EFT is installed), you might want to create a remote connection to remotely administer EFT. Or if you have added a new EFT, you need to configure the new local host.

To specify a new local or remote EFT

1. Do one of the following to open the **New Administrator Connection** wizard:
    - In the **Administrator Login** dialog box that appears when you open the administration interface, click **A remote computer**, and then click **New**.
    - If you are already logged in and want to create a new Server, right-click anywhere on the **Server** tab, and then click **New Server**.
2. Click one of the following:
    - **This computer**
    - **A Remote computer**
3. In the **Label** box, type the name of EFT to which you want to connect.
4. In the **Host address** box, type the IP address of EFT computer.
5. In the **Port** box, type the port number used by EFT.
6. Click **Next**.

    If you close the wizard before the new connection process is complete, none of your settings are saved.

7. After the new host is created, the **Login** dialog box appears. Type your username and password, and then click **Connect**.

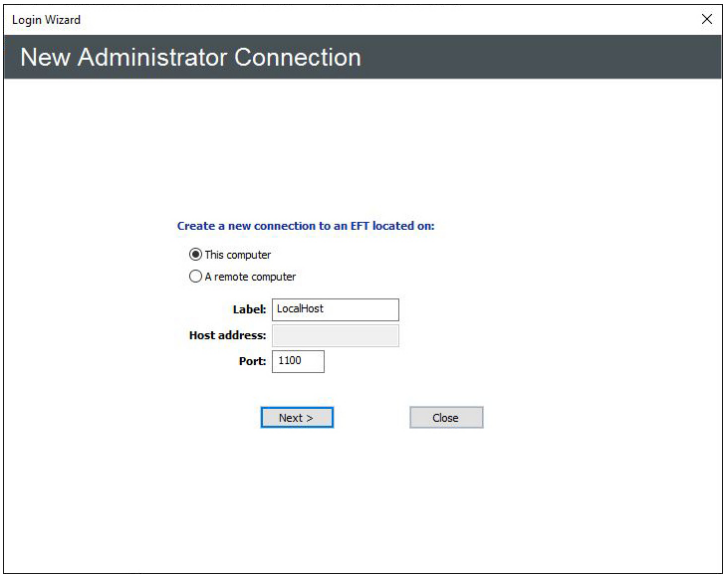
If you are unable to connect to a remote EFT, verify that the remote EFT is configured to allow remote administration, and that you have provided the correct IP address, port, and login information.

New Remote EFT Administration Connection

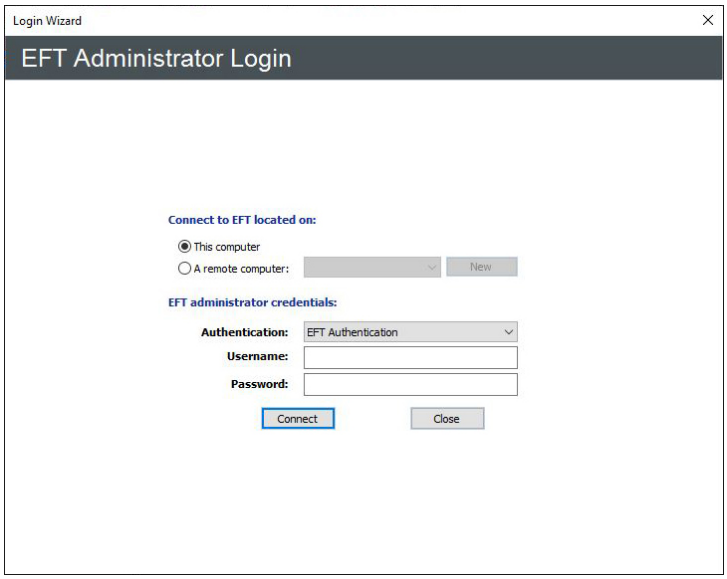
After you have configured a local connection to EFT, you can create a remote connection.

To create a new (remote) EFT administration connection

1. On the main menu click **File >New Server**. The **New administrator Connection** page appears.



2. Be sure that the remote Server service is running, and that it allows remote administration. Then:
    a. Click **A remote computer**.
    b. In the **Label**box, provide a name for the remote Server.
    c. In the **Host address**box, provide the IP address at which the remote Server allows connections.
    d. In the **Port**box, provide the port through which the remote Server allows connections.
3. Click **Next**. The **Login** page appears.



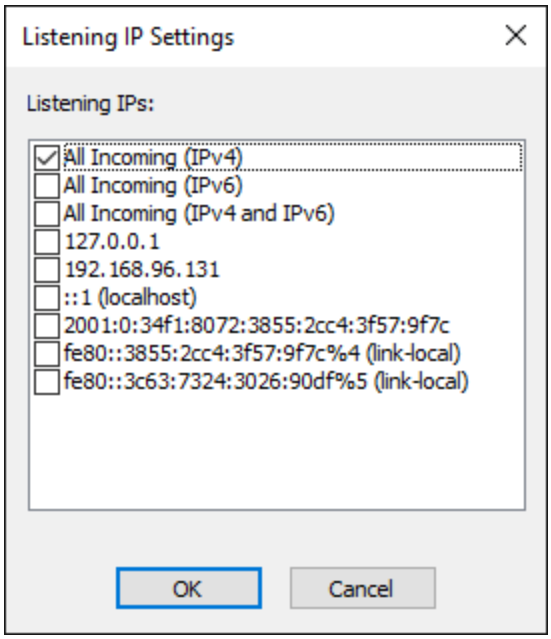
4. Click the **Authentication**box and specify the type of authentication to use for this login. Future connections will default to the authentication type that you specify during this initial login, but you can choose a different type. Authentication types include:
    - **EFT Authentication**- Choose this option to log in with an EFT-specified administrator account, such as the one you created during installation.
    - **Integrated Windows Authentication** - Choose this option to log in as the currently logged on user (Integrated Windows Authentication).
    - **Windows Authentication**- Choose this option to log in using a specific Windows account.
5. If you specified **EFT Server Authentication** or **Windows Authentication**, in the **Username**and **Password** boxes, provide the login credentials that you created during installation. The **Welcome** page appears.

Because you have not yet activated the software, the "Free Trial" reminders appear. After you activate, you will not see this prompt.

6. Do one of the following:
   - If you are evaluating the software or just do not want to activate yet, click **Start Trial**, then follow the procedures in Configuring EFT.
   - If you have purchased a license, click **Activate Now**, then follow the procedures for activating the software.
7. Click **Next**. The **Server Setup** wizard **Welcome** page appears.
8. If you are restoring from a backup, click **Restore from Backup**, then refer to Backing Up or Restoring Server Configuration for the procedure. Otherwise, continue to the next step.
9. If you are not restoring from a backup, click **Next**. The **FIPS Options** page appears.

   When you enable FIPS mode, the ciphers, keys, and hash lengths and types that are not FIPS approved are not available. If a FIPS-approved state cannot be achieved when FIPS is enabled, the EFT service is stopped and an error is written to the Windows Event Log.

   - To use FIPS for SFTP (SSH2), select the **Enable FIPS for SFTP** check box.
   - To use FIPS for SSL, select the **Enable FIPS for SSL** check box.
   - A confirmation prompt appears when you select either check box. When you enable FIPS, the EFT service must be restarted. Click **OK** to continue with FIPS enabled or click **Cancel**if you do not want to use FIPS and restart the EFT service.
10. Click **Next**. The **Remote administration**page appears.
11. Because you are configuring a remote administrator connection, ensure that the **Allow remote administration** check box is selected.
12. Specify the **Listening IPs**.
    a. Click **Configure**to specify one or more IP addresses. The **Listening IP Settings** dialog box appears.



b. **All Incoming (IPv4)** is selected by default. Select the check boxes for addresses that you want to allow; clear the check boxes for the addresses that you do not want to allow, and then click **OK**.

13. Specify the **Listening port**. (For security best practices and compliance with the PCI DSS, specify a port other than the default of 1100.)
14. Click **Next**. The **Secure Remote administration**page appears.
15. Administrator account credentials are transmitted in plain text unless SSL is enabled. Organizations complying with the PCI DSS are required to use SSL for remote administration. To enable secure remote administration, select the **Use SSL for secure remote administration** check box, and then click **Next**. The **SSL Certificate Options** page appears.
16. Do one of the following:
    - In the **Certificate**and **Private Key** boxes, click the folder icon to browse for the private key pair files.
    - Click **Create certificate** to create one. Refer to SSL Certificate-Based Login, Creating Certificates, Importing a Certificate into the Trusted Certificate Database for information regarding certificates.
17. Click **Next**. The **Auditing and Reporting**page appears.
18. If you are using Auditing and Reporting, select the **Enable auditing** check box, then provide the information required to connect to the ARM database as described below. If you are not using Auditing and Reporting, skip to the next step. (Auditing and reporting is a requirement of the PCI DSS.)
    a. In the **Database type** area, specify whether you are using **SQL Server** or **Oracle**for the auditing database.

b. In the **Host[\Instance Name]** box, type EFT name or IP address.

   If you are using SQL Server as the Auditing Database, **\InstanceName** corresponds to SQL Server's notion of named instances, a feature that allows a given computer to run multiple instances of the SQL Server Database Service. For more information, refer to http://msdn2.microsoft.com/en-us/library/ms165614.aspx

c. In the **Authentication**box, specify the type of authentication used by the database, either **Windows Authentication**or **SQL Server Authentication**.
   - If you choose **SQL Server Authentication**, you must also specify the "sa" username and password. In the **Username** and **Password** boxes, type the username and password used to connect to the database (***not***the EFT credentials).

d. In the **Database Name** box, type the name of the database.

e. In the **Audit failure notification email address** box, type the email address to which EFT is to send database connection error notifications. You can add as many email addresses as needed; separate the addresses with a comma or semicolon. EFT uses its global SMTP email settings from the SMTP Configuration to send the emails. You will configure those settings on the next page.

f. In the **In case of audit database error** area, specify an Action for EFT to take if there is an error with the database. To stop recording data, select **Stop auditing**. To continue recording data to a file, select **Audit to folder**, and specify the location for the log file.

   UNC paths are supported. The Globalscape Server service must run on a computer that has access to the network share, and the full UNC path must be used, that is: \\xcvd.forest.intranet.xc\Common_Files, **not** G:\Common.

19. Click **Next**. The specify **SMTP Server Settings**page appears.
20. In the **From email address** box, specify the email address for email notifications (such as those triggered by Event Rules). This is the address that appears in the **From** box of emails sent by EFT. For example, type `noreply@serverhost.com`.
    - The email address is validated when you click **OK**. If the email address contains invalid characters or does not contain the @, an error message appears. Click **OK**to dismiss the error message, then correct the address.
21. In the **SMTP host address** boxes, specify the SMTP server host address and port.

22. If the **Use SMTP server authentication**, select the check box and provide the **Username** and **Password**.
23. Click **Next**. Server Setup is complete.

    You are offered the option of continuing to the Site Setup wizard, or quitting the wizard, saving EFT settings, and configuring the Site(s) later. You must configure at least one Site to service inbound connections to EFT.

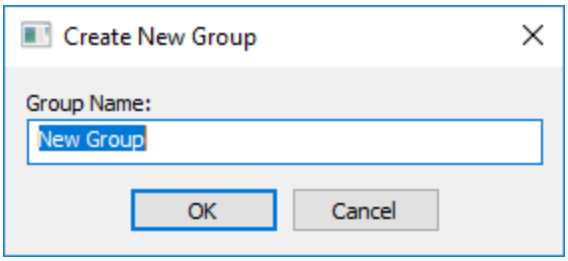
24. Click an option, then click **Finish**. If you chose FIPS mode for SSL and/or SSH, prompts appear explaining that EFT has entered FIPS mode. Click **OK**to dismiss the prompts.
25. If you chose **Run the Site Setup wizard now**, the Site Setup wizard **Welcome** page appears.
26. Refer to Defining Connections to EFT for the procedure for configuring the Site. The procedure differs depending on the user authentication type you choose.

Server Groups

Server Groups are used to organize Servers in the administration interface. They have no effect on the functioning of EFT. The **Default Server Group** is created when you install EFT. You can rename Server Groups, create new Server Groups, and delete Server Groups.

To create a new Server Group

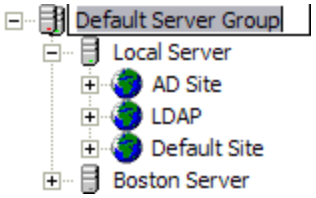
1. In the administration interface, connect to EFT and click the **Server** tab.
2. Click **File >New Server Group**. The **Create New Group** dialog box appears.



3. In the **Group Name**box, type a descriptive name for the Server Group. The name will appear in the tree and in reports and log files.
4. Click **OK**.

To rename a Server Group

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server Group you want to rename.
3. On the menu bar, click **Configuration >Rename Selected**(or press F2).



4. Next to the Server Group's icon, type a different name.
5. Press ENTER.

To delete a Server Group

You can only delete a Server Group if more than one is defined.

1. In the administration interface, connect to EFT and click the **Server** tab.
2. Click the Server Group that you want to delete.

3. Do one of the following:
    - On the main menu, click **File >Remove Server Group**.
    - Right-click the Server Group, and then click **Remove Server Group**.

Related Topic

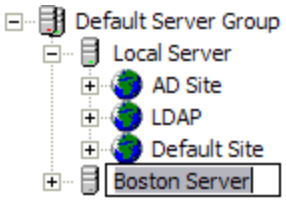
- Permission Groups (not the same as a Server Group)

Renaming, Deleting, and Moving a Server

In the administration interface, you can rename and delete a Server, and move a Server to a different Server Group. When you delete a Server or Server group, you remove all of its login and configuration information. You can no longer connect to EFT if you delete it or its Server Group.

To rename a Server

1. In the administration interface, connect to EFT and click the **Server** tab.
2. In the left pane click the Server node you want to rename.
3. On the menu bar, click **Configuration>Rename Selected** (or press F2).



4. Next to the Server's icon, type a different name.
5. Press ENTER.

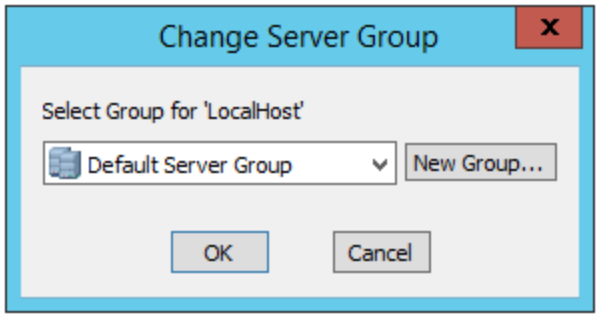
To delete a Server

When you delete a Server, you also delete all of its login information. You cannot undo this action.

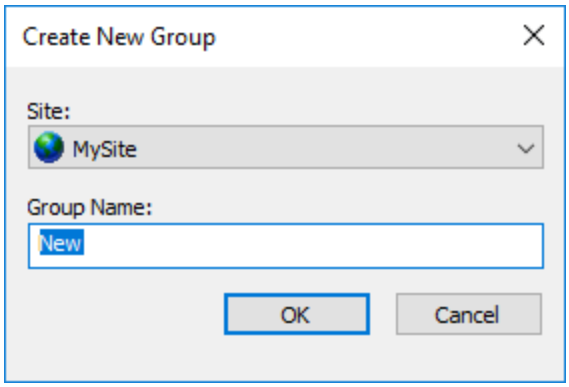
1. In the administration interface, connect to EFT and click the **Server** tab.
2. Do one of the following:
   - Right-click the Server node you want to delete, then click **Remove Server**.
   - Click the Server you want to delete, then on the main menu, click **File >Remove Server**.
3. A warning message appears. In the **Password**box, type the EFT administrator password, and then click **Delete**.

To move a Server to a different Server Group

1. In the administration interface, click the **Server**tab.
2. Right-click the Server node you want to move, then click **Change Server Group**. The **Change Server Group** dialog box appears.



3. Do one of the following:
   - If the Server Group is defined, click the **Select Group** drop-down menu to select the Group.
   - If the Server Group is not defined:
     a. Click **New Group**. The **Create New Group** dialog box appears.



     b. Type a name for the new group, and then click **OK**. The **Change Server Group** dialog box reappears.
4. Click **OK**.

Related Topic

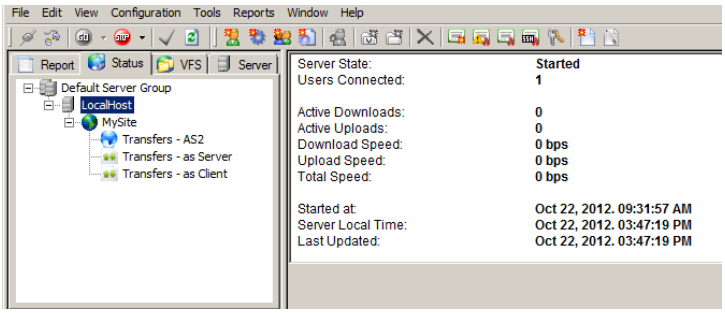
- Permission Groups (not the same as a Server Group)

Monitoring Connections to EFT

EFT can monitor user's FTP/SFTP connections in real time, display the information in the administration interface, and record the activity to a log.

To monitor a user connection

1. In the administration interface, connect to EFT, and click the **Status** tab.
2. In the left pane, click the server node.



3. The right pane shows the number of users connected to the Server, information about transfers, and server connection time.

Related Topics

- Viewing Transfers To and From the Site
- Viewing Connections to a Site
- Server Statistics
- Status Tab
- Forcibly Logging a User Off of EFT
- AS2 Transaction Auditing and Monitoring
- Resubmitting AS2 Transmissions

EFT Messages and Templates

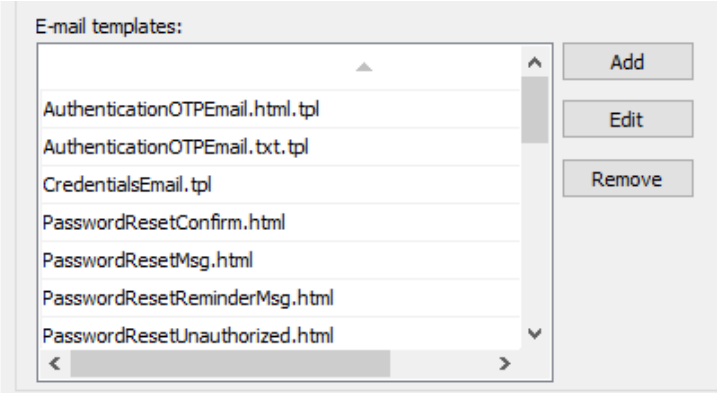
EFT generates several different types of messages during operation, such as event rule actions and server-level notifications. Some messages can be edited within the administration interface, others must be edited within a text file that you create, and others are hard coded and not editable. The various messages and their uses are described below.

The **Templates** directory listed below is in the shared configuration directory for clusters, or **\ProgramData\Globalscape\EFT Server\Templates**. Templates can be either HTML, TXT, or TPL, and all can be edited in a text editor.

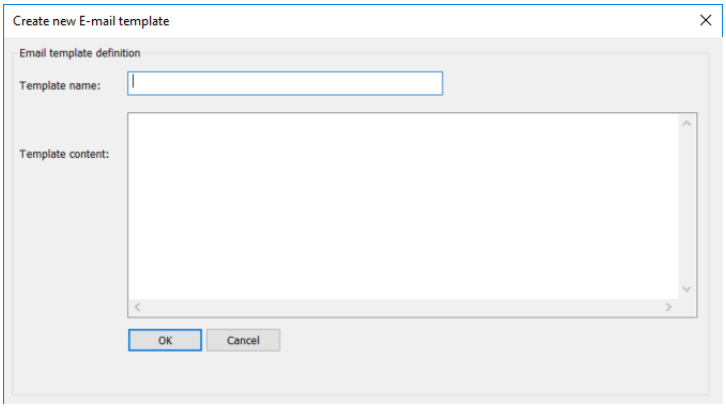
- EFT standalone template files were moved from the root of the local config directory to the "Templates" folder of the same location.
- EFT HA template were files moved from the root of each node's local config directory to the "Templates" folder in the shared config directory. All nodes' now share a single copy of each template, instead of having their own copy locally.
- Templates stored in the "HTTPMessages" folder have also moved to the "Templates" folder for both standalone and HA.
- Upon upgrade from previous EFT versions to 8.1.0.11, new templates are created and old templates are moved to the local **config\Backup\Templates Backup...** directory. Therefor any customization to these templates will be lost on upgrade but are backed-up.

Email Templates on the Server > SMTP Tab

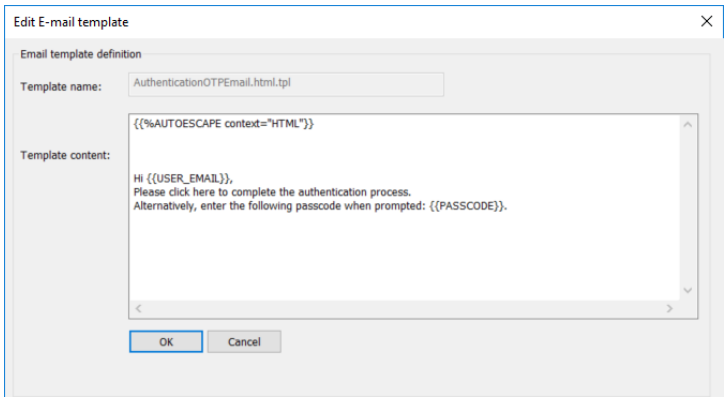
At the bottom of the **SMTP** tab is a table listing the email templates that you can edit or remove as well as add new templates.



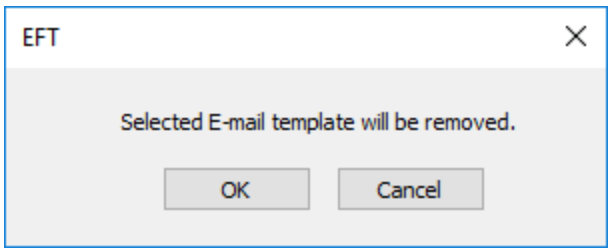
Add - Click **Add** to add a template. You can use HTML or plain text, and context variables and environment variables (with curly {{ }} brackets). View the existing templates for examples.



Edit - Click **Edit** to edit a selected template. Avoid deleting or changing any of the context variables and environment variables (with curly {{ }} brackets) that EFT uses. You can use HTML or plain text.



Remove - Click **Remove** to remove a selected template. A message appears to confirm that you want to remove the template.



The Templates directory contains the following templates:

- AuthenticationOTPEmail.html.tpl or AuthenticationOTPEmail.txt.tpl - Sent for two-factor authentication in the send and reply portals
- BAD_PARAMETER.htm - HTTP/1.1 406 Bad Parameter; The requested URL was not found on this server.
- BAD_REQUEST.htm - HTTP/1.1 400 Bad Request
- BAD_URI.htm -
- CONFLICT.htm - HTTP/1.1 409 Conflict
- CredentialsEmail.tpl - Sent when account credentials are created or modified.
- FORBIDDEN.htm
- INSUFFICIENT_STORAGE.htm
- INTERNAL_SERVER_ERROR.htm
- LENGTH_REQUIRED.htm
- MAPPER_DENIED_ACCESS.htm
- MAX_QUOTA_REACHED.htm
- NOT_FOUND.htm
- NOT_IMPLEMENTED.htm

- PasswordResetConfirm.html - Sent when a user requests a password reset--applies to all users on the Server; but you can create Site-specific versions, as described at the link.
- PasswordResetMsg.html - Notifies users after their password has expired
- PasswordResetReminderMsg.html - Notifies users of their pending password expiration up to 30 days prior to the password expiration date
- PasswordResetUnauthorized.html - Sent when a password change is requested but EFT has disabled password reset for the account
- PATH_TOO_LONG.htm
- PGPKeyExpirationError.txt - The key with fingerprint or ID: %keyid% expired on %expirationdate%
- PGPKeyExpirationWarning.txt - The key with fingerprint or ID: %keyid% is set to expire %d% day(s) from now on %expirationdate%
- PRECONDITION_FAILED.htm
- REQUEST_TOO_LARGE.htm
- SERVICE_UNAVAILABLE.htm
- SSLCertExpirationError.txt - The SSL certificate: %certid% expired on %expirationdate%.
- SSLCertExpirationWarning.txt -The SSL certificate: %certid% is set to expire %d% day(s) from now on %expirationdate%.
- URI_TOO_LARGE.htm
- UsernameResend.txt - Sent when a user requests the account username.
- WorkspaceNotification.txt - When a user shares a folder, an invitation is sent to the user with whom the folder is shared. If the recipient does not have an account on EFT, the user can register the account.
- WorkspacesAdminAddedParticipantMsg.html - When an administrator adds a participant to a shared workspace via the VFS tab in the administration interface, an email is sent to the user with a link to the workspace, along with the folder name and Workspace owner name.
- WorkspacesInviteRegisterMsg.html - When a Workspace owner invites a user to join the workspace, an invitation is sent to the user with the Workspace owner's name and folder name.
- WorkspacesInviteVerifyMsg.html - After a user has accepted the Workspace share invitation, EFT sends an account verification request.
- WorkspacesOAIEmail.html, WorkspacesOAIEmail.txt, WorkspacesOAIEmailWithSecureMB.html, WorkspacesOAIEmailWithSecureMB.txt - When a user sends a file to another users via the EFT Outlook Add-In, EFT sends an email with a link to the

Workspace location, rather than the actual file.

- WorkspacesRequestFileEmail.html.tpl, WorkspacesRequestFileEmail.txt.tpl - {{SENDER}} has requested a file from you{{#SHOW_REPLY_ALL}} and others {{/SHOW_REPLY_ALL}}.

Refer to the table for more information. about EFT messages:

Message	Description	
Audit failure notification email	Sent when database connection errors occur	System message; not editable
Connection Banner Message	When a client first connects to the Site via FTP, but before the user logs on, the connection banner appears.	Administration interface, Site > **Connections** tab > **FTP/S Config** > **FTP Settings** dialog box
Email Notification Message	Email sent with the **Send Mail** Action when an Event Rule is triggered.	Administration interface, **Server node > Event Rules node > Event Rule**
Invalid parameter count message	Sent when the number of parameters provided to execute a Custom command is not the correct number of parameters.	Administration interface, **Command Settings** tab of a selected Command, in the **FTP Custom Command Specific** dialog box.
Quit Session Messages	Message that appears when the client closes the session gracefully by using the FTP QUIT command.	Administration interface, Site > **Connections** tab > **FTP/S Config** > **FTP Settings**dialog box
SSL Certification expiration warnings	Sent when SSL certificate is about to expire in *n* days, and when the certification has expired.	Administration interface, **Site > Connections** tab > **SSL certificate settings**, **Configure** > **Expiration Notification** > **Configure** > **Certificate Expiration Notification** dialog box.
User Limit Reached Message	Message that appears to the user when the maximum simultaneous connections limit is exceeded	Administration interface, Site > **Connections** tab > **FTP/S Config** > **FTP Settings**dialog box
Workspaces OAI Email sent	When a user sends a file to another users via the EFT Outlook Add-In, EFT sends an email with a link to the Workspace location, rather than the actual file.	EFT looks for the file WorkspacesOAIEmail.html, WorkspacesOAIEmail.txt, WorkspacesOAIEmailWithSecureMB.html, WorkspacesOAIEmailWithSecureMB.txt in the **\Template** directory.
Workspaces Request File	When a user requests a file from another user, EFT sends a request file message.	EFT looks for the file WorkspacesRequestFileEmail.html.tpl, WorkspacesRequestFileEmail.txt.tpl in the **\Template** directory.

Message	Description	
WTC login error message	When a user provides the wrong username and/or password, the message "Not logged in" appears. The message is purposefully vague for security.	Hard-coded and not customizable. (Forgot username and Forgot password links allow the user to request assistance.)

EMAIL TEMPLATE VARIABLES

The available variables for each template (on the **Server > SMTP** tab and \ProgramData\Globalscape\EFT Server\Templates\) are indicated below with a check mark.

	Workspaces							OTP	Admin UI	WTC Login			Password Manage-ment		PGP		
Variable	WorkspaceNotification.txt	WorkspacesAdminAddedParticipantMsg	WorkSpacesInviteRegisterMsg	WorkSpacesInviteVerifyMsg	WorkspacesOAIEmail.html|txt	WorkspacesOAIEmailWithSecureMB.html|txt	WorkspacesRequestFileEmail.html.tpl	AuthenticationOTPEmail.html|txt (OTP - Email Delivery)	CredentialsEmail.tpl	UsernameResend.txt	PasswordResetConfirm.html	PasswordResetUnauthorized.html	PasswordResetMsg.html	PasswordResetReminderMsg.html	PGPKeyExpirationError	PGPKeyExpirationWarning.txt	Description
%WS_OWNER_NAME%		✓	✓														Workspace owner display name (sender's username)
%FOLDER_NAME%		✓															
%WS_FOLDER_NAME%	✓		✓														Workspace folder name
%FILE_ACTION%	✓																
%RECIPIENT%	✓																Workspace recipient's email address
%RECIPIENTS%					✓	✓											Workspace recipient's email addresses
%RECIPIENT_IP%	✓																Workspace recipient's remote IP address
%CC_RECIPIENTS%					✓	✓											
%ACTION_DATE%	✓																
%ACTION_TIME%	✓																

EMAIL TEMPLATE VARIABLES

	Workspaces							OTP	Admin UI	WTC Login			Password Manage-ment		PGP		
Variable	WorkspaceNotification.txt	WorkspacesAdminAddedParticipantMsg	WorkSpacesInviteRegisterMsg	WorkSpacesInviteVerifyMsg	WorkspacesOAIEmail.html|txt	WorkspacesOAIEmailWithSecureMB.html|txt	WorkspacesRequestFileEmail.html.tpl	AuthenticationOTPEmail.html|txt (OTP - Email Delivery)	CredentialsEmail.tpl	UsernameResend.txt	PasswordResetConfirm.html	PasswordResetUnauthorized.html	PasswordResetMsg.html	PasswordResetReminderMsg.html	PGPKeyExpirationError	PGPKeyExpirationWarning.txt	Description
%USER.LOGIN%		✓	✓							✓	✓	✓	✓				Username
%USER.FULL_NAME%										✓		✓	✓	✓			User Full Name
%USER.EMAIL_ADDRESS%			✓	✓													User email address
%LINK%		✓	✓	✓							✓						Link Domain + Link Path
%LINK_DOMAIN%			✓	✓													Link Domain
%LINK_PATH%			✓	✓													Workspace link path
%WS_MESSAGE%		✓	✓														Workspace Comment
%VERIFICATION_LINK%				✓													Invitation verification link
%PASSCODE%				✓													One time passcode
%WORKSPACE_LINK%					✓												Workspace link. Includes a href.
%DATE_EXPIRE%					✓	✓											Workspace Expiration date
%FILE_LINK%																	
%FILE_SMART_SIZE%																	
%SITE.ACCOUNT_MANAGEMENT_URL%													✓	✓			Site's account management URL

EMAIL TEMPLATE VARIABLES

	Workspaces							OTP	Admin UI	WTC Login			Password Manage-ment		PGP		
Variable	WorkspaceNotification.txt	WorkspacesAdminAddedParticipantMsg	WorkSpacesInviteRegisterMsg	WorkSpacesInviteVerifyMsg	WorkspacesOAIEmail.html|txt	WorkspacesOAIEmailWithSecureMB.html|txt	WorkspacesRequestFileEmail.html.tpl	AuthenticationOTPEmail.html|txt (OTP - Email Delivery)	CredentialsEmail.tpl	UsernameResend.txt	PasswordResetConfirm.html	PasswordResetUnauthorized.html	PasswordResetMsg.html	PasswordResetReminderMsg.html	PGPKeyExpirationError	PGPKeyExpirationWarning.txt	Description
%DAYS_LEFT%														✓			Days left before user's password expire
%REMOTE_IP%											✓	✓					User's remote IP address
%keyid%															✓	✓	PGP key name/id
%d%															✓	✓	Number of day(s) to expire from now
%expirationdate%															✓	✓	PGP expiration date
%s%											✓						Minutes before reset link expire
{{SENDER}}							✓										Sender's request file
{{REPLY_URL}}							✓										Request file reply URL
{{EXPIRE_TIME}}							✓										Request file expiration time
{{SENDER_MESSAGE}}							✓										Request file message
{{USER_EMAIL}}								✓									User email address
{{LINK}}								✓									Verification link (OTP)
{{PASSCODE}}								✓									One time passcode

EMAIL TEMPLATE VARIABLES

	Workspaces							OTP	Admin UI	WTC Login			Password Manage-ment		PGP		
Variable	WorkspaceNotification.txt	WorkspacesAdminAddedParticipantMsg	WorkSpacesInviteRegisterMsg	WorkSpacesInviteVerifyMsg	WorkspacesOAIEmail.html|txt	WorkspacesOAIEmailWithSecureMB.html|txt	WorkspacesRequestFileEmail.html.tpl	AuthenticationOTPEmail.html|txt (OTP - Email Delivery)	CredentialsEmail.tpl	UsernameResend.txt	PasswordResetConfirm.html	PasswordResetUnauthorized.html	PasswordResetMsg.html	PasswordResetReminderMsg.html	PGPKeyExpirationError	PGPKeyExpirationWarning.txt	Description
{{USER_FULL_NAME}}									✓								User's full name
{{USER_LOGIN}}									✓								User's login username
{{USER_PASSWORD}}									✓								User's password
{{WEB_PORTAL_DOMAIN}}									✓								Domain specified in site's Send Portal dialog
{{WEB_PORTAL_PORT}}									✓								Port specified in site's Send Portal dialog, hardcoded value must be preceded by ':'
{{MTCURL}}									✓								Encoded credentials for use with mobile client
{{MTC_LINK_ALT}}									✓								Alternate version of MTCURL for certain scenarios

File Locations

EFT installs/stores its files in the following locations:

- EFT configuration is stored in DB files(for example, Serverconfig.db)
- Main program files are installed in:
  - **C:\Program Files\Globalscape\EFT Server**
- Application data.
  - **C:\ProgramData\Globalscape\EFT Server**
  - EFT stores its data in a hidden folder named **C:\ProgramData**. (To show **\ProgramData**in Windows File Explorer, click **View**tab > **Hidden**items.)
- EFT client operational files are stored in <EFT installation folder>**\Web**for a stand-alone installation.
- The WTC user folders and files are stored:
  - In non-HA installations, on the EFT computer (for example, **C:\InetPub\EFTRoot\MyGSSite\Usr**).
  - In HA installations, in the shared HA configuration location (for example, <NAS_drive>\<HA config folder>**\InetPub\EFTRoot\MyGSSite\Usr**).

Encryption Algorithms

The topics below list the encryption algorithms available in EFT, OpenPGP, and the Advanced Workflows. It is up to you to determine which settings to use in your environment.

- SSL Encryption Algorithms
- SFTP Encryption Algorithms
- OpenPGP Encryption Algorithms
- Old Algorithms Removed

Old Algorithms Removed

This topic lists which algorithms were removed from EFT and which are the default.

The following algorithms were removed/ desupported in v8.0.5:

TLS_AES_256_GCM_SHA384

TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

ECDHE-ECDSA-CHACHA20-POLY1305

ECDHE-RSA-CHACHA20-POLY1305

DHE-RSA-CHACHA20-POLY1305

ECDHE-ECDSA-AES256-CCM8

AES256-CCM8

ECDHE-ECDSA-AES256-CCM

DHE-RSA-AES256-CCM

AES256-CCM

ECDHE-ECDSA-ARIA256-GCM-SHA384

ECDHE-ARIA256-GCM-SHA384

DHE-RSA-ARIA256-GCM-SHA384

DHE-DSS-ARIA256-GCM-SHA384

ARIA256-GCM-SHA384

ECDHE-ECDSA-AES128-CCM8

DHE-RSA-AES128-CCM8

AES128-CCM8

ECDHE-ECDSA-AES128-CCM

DHE-RSA-AES128-CCM

AES128-CCM

ECDHE-ECDSA-ARIA128-GCM-SHA256

ECDHE-ARIA128-GCM-SHA256

DHE-RSA-ARIA128-GCM-SHA256

DHE-DSS-ARIA128-GCM-SHA256

ARIA128-GCM-SHA256

ECDHE-ECDSA-CAMELLIA256-SHA384

ECDHE-RSA-CAMELLIA256-SHA384

DHE-RSA-CAMELLIA256-SHA256

DHE-DSS-CAMELLIA256-SHA256

ADH-CAMELLIA256-SHA256

CAMELLIA256-SHA256

ECDHE-RSA-CAMELLIA128-SHA256

DHE-RSA-CAMELLIA128-SHA256

DHE-DSS-CAMELLIA128-SHA256

ADH-CAMELLIA128-SHA256

CAMELLIA128-SHA256

DHE-RSA-DES-CBC3-SHA

DHE-DSS-DES-CBC3-SHA

DHE-RSA-AES256-CCM8

ECDHE-ECDSA-CAMELLIA128-SHA256

The following 25 ciphers are enabled by default:

TLS_AES_256_GCM_SHA384

ECDHE-ECDSA-AES256-GCM-SHA384

ECDHE-RSA-AES256-GCM-SHA384

AES256-GCM-SHA384

TLS_CHACHA20_POLY1305_SHA256

ECDHE-ECDSA-CHACHA20-POLY1305

ECDHE-RSA-CHACHA20-POLY1305

TLS_AES_128_GCM_SHA256

ECDHE-ECDSA-AES128-GCM-SHA256

ECDHE-RSA-AES128-GCM-SHA256

AES128-GCM-SHA256

ECDHE-ECDSA-AES256-CCM8

AES256-CCM8

ECDHE-ECDSA-AES256-CCM

AES256-CCM

ECDHE-ECDSA-AES128-CCM8

AES128-CCM8

ECDHE-ECDSA-AES128-CCM

AES128-CCM

ECDHE-ECDSA-AES256-SHA384

ECDHE-RSA-AES256-SHA384

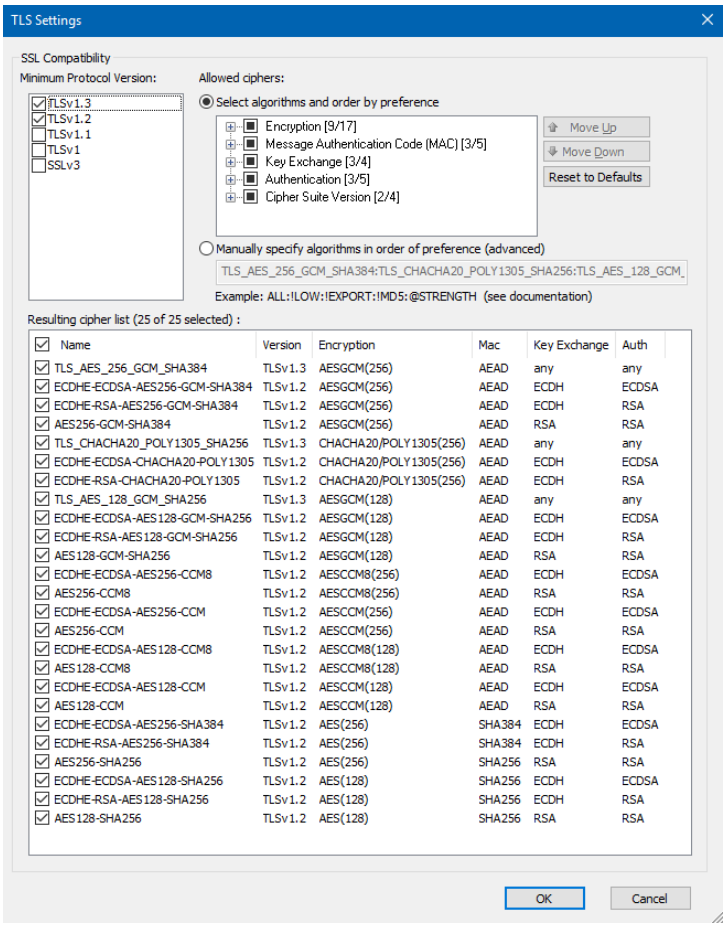
AES256-SHA256

ECDHE-ECDSA-AES128-SHA256

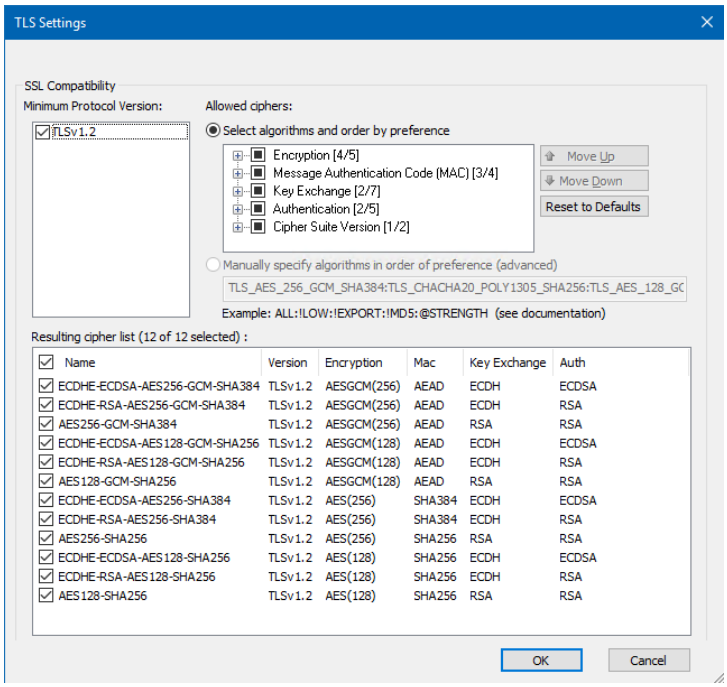
ECDHE-RSA-AES128-SHA256

AES128-SHA256

Default Settings for SSL TLS:



FIPS mode was unchanged:



IPv6 Support in EFT

EFT supports IPv6 connections. You can continue to use IPv4 addresses, only IPv6 addresses, or a both IPv4 and IPv6. All IP address fields accept IPv4, IPv6, and host names transparently; you are not required to understand what an IPv4 or IPv6 address is to use it. Outbound connections are handled transparently based on the IP address or host entered into any host fields. EFT determines whether the connection requires IPv4 or IPv6 without requiring you to specify.

IPv6 is not supported in EFT HA environments.

The following areas of EFT support IPv6 addresses:

- Configuring EFT - The Server's listening IP address and the IP address used for remote administration each support IPv6 addresses.
- Defining Connections (Sites) - The Site's listening IP address supports IPv6 addresses.
- IP ban/access rules - The IP address ban/access rules support IPv6 addresses. (Refer to Controlling IP Access for Remote administration and Controlling Access to the Site by IP Address for information about banning IP addresses.)
- Event Rules - The Copy/Move Action and the Download Action support IPv6 address. When you create an Event Rule using one of these actions, you can specify an IPv4 or IPv6 address or let EFT choose the best available address to use.
- Various COM API objects have been modified to allow the use of IPv6 addresses, and new methods were added to support multiple listening IP addresses.
- DMZ Gateway was updated to allow both IPv4 and IPv6 addresses.
- The Auditing and Reporting module schema has been modified to allow IPv6 addresses.
- The AS2 modulesupports both IPv4 and IPv6 addresses.
- IPv6 addresses use colons, but a colon is not a valid character in UNC path names. To address this, Microsoft created the "ipv6-literal.net" domain. An IPv6 literal address is an ipv6-address with the colon ':' characters replaced by dash '-' characters, and then followed by the ".ipv6-literal.net" string.

  For example, for the following IPv6 address:

  ```
  2001:4898:9:3:c069:aa97:fe76:2449
  ```

  would be translated as follows:

```
\\2001-4898-9-3-c069-aa97-fe76-2449.ipv6-literal.net\share
```

For more information about the ipv6-literal.net domain, refer to the MSDN article at http://msdn.microsoft.com/en-us/library/aa385353.aspx.

- CIDR notation is supported for both IPv4 and IPv6 literals. For example: 2001:cdba:9abc:5678::/64 for blocking an IPv6 LAN or 192.168.29.0/24 for an IPv4 network.

IPv6 FAQ

Q. What is IPv6?

A. IPv6 is a proposed replacement to IPv4. One of the benefits of IPv6 is a larger address space, with 128 bits versus IPv4's 32 bits. Search online to learn more about IPv6, the benefits it provides, and challenges it presents.

Q. When will IPv6 replace IPv4?

A. This is the subject of much debate. Many have claimed for years that we are in imminent danger of running out of IPv4 addresses; however, NATing (including ISP carrier grade NATing) and other workarounds have surfaced that will delay the inevitable exhaustion of IPv4 address for at least a few more years.

Q. If the need for IPv6 is not imminent, then why was it incorporated into EFT?

A. Large enterprises are leading the way in converting to IPv6 (at least internally) and EFT is often a critical piece of the edge architecture for many of these companies. Also, our government customers are actively transitioning to IPv6 based on internal mandates and have requested support for IPv6.

Q. Is IPv6 supported limited to EFT? Or does it include the DMZ Gateway as well?

A. EFT and the DMZ Gateway comprehensively support IPv6. DMZ Gateway requires Windows Server 2008 for IPv6. (In Windows 2003, IPv6 is not supported for DMZ Gateway.)

Q. Will EFT operate with a mix of IPv4 and IPv6 addresses?

A. EFT supports the three scenarios (abstract network topologies) described in RFC 4057, in addition to the current IPv4-only scenario. The scenarios include 1) dual-stack, which is the wide-scale deployment of hosts that support both IPv4 and IPv6 running simultaneously; 2) sparse dual stack, in which only some applications in the infrastructure support IPv6 (mainly during the transition to full dual stack or IPv6 only); and 3) IPv6 only, in which all nodes in the infrastructure operate exclusively on IPv6.

Q. How is dual stack possible given that EFT currently supports only “all incoming” or a single listener IP address?

A. You can choose a single listener IP address, all incoming IPv4 addresses, all incoming IPv6 addresses, all incoming IPv4 and IPv6 addresses, or multiple specific IPv4 and/or IPv6 addresses for the Site and/or administration listeners.

Q. If EFT and DMZ Gateway are working in a pure IPv6 environment, how will they correspond with the outside world, parts of which are still using IPv4?

A. DMZ Gateway's server support for IPv6 was ingeniously implemented so that it can act as a 4to6 or 6to4 translator. For example, DMZ Gateway can listen on IPv4 IPs for incoming connections, but then route those to IPv6 listeners in EFT. Likewise, it can broker IPv6-initiated connections from EFT to external hosts located on IPv4 networks.

Q. Is EFT backward compatible with prior versions of the DMZ Gateway?

A. Yes. For IPv6 support, you will need to upgrade to DMZ Gateway v3.2 or later.

Q. Is IPv6 support available by default when newly installed?

A. Yes, IPV6 support is available by default. However, on dual stack systems, IPv6 listener IPs are not selected by default. To comply with Department of Defense requirement 5.3.5.4, 1.2 (all nodes and interfaces that are IPv6 capable must be carefully configured and verified prior to enabling/using IPv6), it is up to the administrator to configure which IPv6 addresses to use as the listener, rather than the default "All incoming IPv4" selection (if IPv6 support is required).

Q. How does EFT support IPv6 for FTP connections, given the need for separate control and data channels?

A. EFT (as both server and client) fully complies with RFC 2428 for client-initiated negotiation of extended port (EPRT) and extended passive (EPSV) data connection modes. Furthermore, EFT complies with draft-ietf-ftpext2-ftp64-00, an ingenious solution to a scenario in which a pure IPv6 client connects to an IPv4 server over a 6to4 translator, but receives an error in response to the EPSV command (unsupported by the IPv4 server). In that case, EFT reverts to sending the PASV command to obtain the port number, but then uses the host’s IPv6 address as the data connection address, ignoring the IPv4 address returned because of the PASV command.

Q. Can EFT audit or log IPv6 addresses?

A. Yes. EFT can both audit and report IPv6 addresses, including the file transfer status viewer and anywhere else IP addresses are displayed or saved in the program. Note that IPv6 addresses are displayed in the administration interface, status viewer, and reports using shorthand form to conserve space (according to section 3 of RFC 1924).

The exception to this rule is in the DMZ Gateway, which uses the preferred form (also documented in section 3 of RFC 1924).

Q. Can EFT connect to my SMTP server, LDAP, or AD for the authentication provider or the ARM SQL Server if they are on an IPv6 network?

A. As long as the remote system or component is addressable via IPv6, you can specify an IPv6 address and EFT will connect to the IPv6 host.

Q. How does IPv6 affect upgrades or backup-and-restore functions?

A. The current Site/administrator listeners will be respected and warnings will occur if their IP addresses are no longer present. Existing COM scripts will not be affected. When restoring from a backed up configuration, the specified listener IP addresses are conserved; however, you will be given the option to specify new listeners, including IPv6 addresses (if present), or a mix of IPv4 and IPv6 addresses.

Q. Does EFT's ban list work with IPv6 IP addresses?

A. DoS and Flood protection work regardless of protocol, along with all controls related to managing IP ban lists. What's more, EFT now supports CIDR Classless Inter-Domain Routing (CIDR) for IP masking for banned IPv4 and IPv6 addresses, meaning you can now specify masks such as 255.255.29.0/24 or 2001:cdba:9abc:5678::/64 instead of wildcard masking, although wildcards are still supported for IPv4 address masking for legacy users.

Q. How does EFT know whether the host address supplied for a remote connection is IPv4 or IPv6?

A. In accordance with RFC 3484, EFT will use address look-up to determine the family and correct connection type without asking the administrator for more information. Address look-up will result in a list of addresses ordered by most preferred. EFT will then attempt to connect to each address in order until a successful connection occurs or that list is exhausted, and will log the result in the EFT debug log. Keep in mind that you can enter an IPv4, IPv6, or host address anywhere an address can be entered. The only exceptions are fields that cannot take host addresses, such as the Site listener IP.

Q. When specifying multiple IP addresses, which source IP address is used for binding when making an outbound connection as part of an Event Rule sequence?

A. EFT can automatically choose the IP address (it selects from the top of adaptor order using whatever internal mechanisms Windows uses) or the administrator can specify the source IP address.

Q. What if I'm not using or don't care about IPv6? Will I notice any change?

A. We have made IPv6 support as unobtrusive as possible. Pure IPv4 customers will not be affected and will not see any UI or other changes. A difference will only be noticed once/if IPv6 adaptors are physically enabled on the system.

Q. What about COM support for IPv6?

A. New methods have been created to fully support IPv6, while legacy methods have been retained for backward compatibility. (Refer to the COM API referencefor details.)

IDN Support in EFT

The Domain Name System (DNS) is restricted to the use of up to 63 ASCII characters. An internationalized domain name (IDN) is an Internet domain name that contains at least one label (for example, www, globalscape, and com are each *labels*) that is displayed in a language-specific script or alphabet, such as Chinese, Russian, or the Latin alphabet-based characters with diacritics, such as French. These writing systems are encoded in multi-byte Unicode. Internationalized domain names are stored in the DNS as ASCII strings using Punycode transcription. (Punycode encoding syntax is defined in RFC 3492, Punycode: A Bootstring encoding of Unicode Internationalized Domain Names in Applications (IDNA).)

The table below describes IDN support in EFT.

Product	Field	GUI Accepts	GUI Displays	Usage	Stored as
EFT	All domain (host) fields	Unicode or ASCII	Unicode	Punycode	Unicode
EFT	All email fields (for example, imauser@me.com)	ASCII only (7-bit)	ASCII	ASCII	Unicode
EFT	Email usernames (for example, Ima User)	Unicode	Unicode	Unicode	Unicode

Related Topic

- Unicode Support in EFT

Erasing EFT Configuration

If you want to completely remove EFT configuration (Servers, Sites, Settings Templates, and users), you can do so with the procedure below.

To erase EFT configuration

1. Stop the Server service.
2. Delete configuration files in the EFT installation directory (for example, **C:\ProgramData\Globalscape\EFT Server**).
3. Start the Server service.
4. Launch the administration interface and log in with the username and password used during installation of EFT.
5. Recreate your Sites, Settings Templates, and users (all are removed when you delete the configuration files).

HA (Active-Active) Deployments

The topics below cover High Availability (active-active) deployments.

- High Availability Overview
- HA FAQ
- Non-High Availability Mode vs. High Availability Mode
- Active-Active HA Cluster--Installing or Upgrading the Server
- Upgrade an HA Cluster with Zero Downtime
- High Availability Tab of a Server
- High Availability Message Queuing
- HA Nodes Configuration File
- Node Discovery using Shared Storage for HA Clusters
- EFT Deployment Scenarios
- Server Drain, Maintenance, and Auto-Restart
- Unicast
- Viewing Node Status
- Logging for HA Nodes
- HA-Related Knowledgebase Articles

High Availability Overview

EFT High Availability (HA) solution can protect your critical business processes and ensure that crucial file transfer systems are always on, and that employees, customers, and business partners experience seamless availability of critical applications and information.

EFT with HA can:

- Maintain availability through any planned or unplanned outage
- Increase stability and flexibility by implementing multiple nodes of EFT for load balancing
- Enhance throughput and better meet important SLAs by deploying multiple nodes of EFT to allow the collective environment to use more available resources
- Improve scalability with the ability to share common configurations across nodes, eliminating the challenge of having multiple servers set up with different configurations

EFT's active-active deployment provides HA using multiple instances of EFT and a load balancer for non-stop availability of your network. And unlike active-passive failover clusters, all of the nodes in EFT's active-active deployment are put to work in production—with no standby hardware, and no clustering software.

Interoperable with Common Load Balancers

With EFT HA, you can control spikes in network traffic, minimize scalability limitations, and maximize the efficiency of large and complex environments. Globalscape's high availability solution is compatible with most major load balancers.

In addition, Globalscape is a member of the F5®Technology Alliance Program, providing a proven managed file transfer solution for interoperability of F5 BIG IP® Local Traffic Manager™ (BIG-IP LTM®) with Globalscape's managed file transfer platform, Enhanced File Transfer™ (EFT™) with High Availability (HA), to secure enterprise data at rest and in transit, without interruption.

What's the difference between active-active and active-passive load balancing?

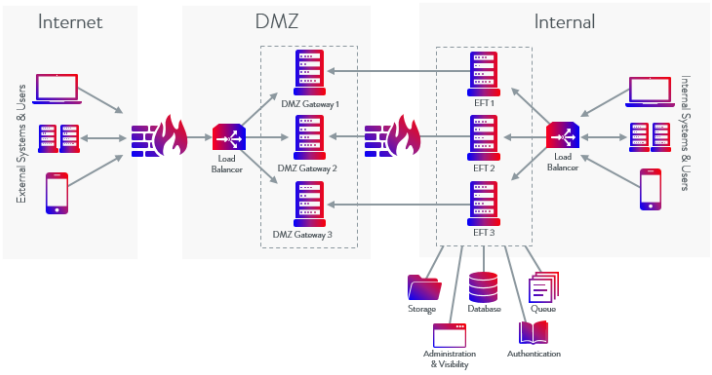
- An active-active cluster is typically made up of at least two nodes, both actively running the same kind of service simultaneously. The main purpose of an active-active cluster is to achieve load balancing. Load balancing distributes workloads across all nodes to prevent any single node from getting overloaded. Because there are more nodes available to serve, there will also be a marked improvement in throughput and response times.
- Like the active-active configuration, active-passive also consists of at least two nodes. However, as the name "active-passive" implies, not all nodes are going to be active. In the case of two nodes, for example, if the first node is already active, the second node must be passive or on standby. The passive (a.k.a. failover) server serves as a backup that's ready to take over as soon as the active (a.k.a. primary) server gets disconnected or is unable to serve.

Cluster Types Supported

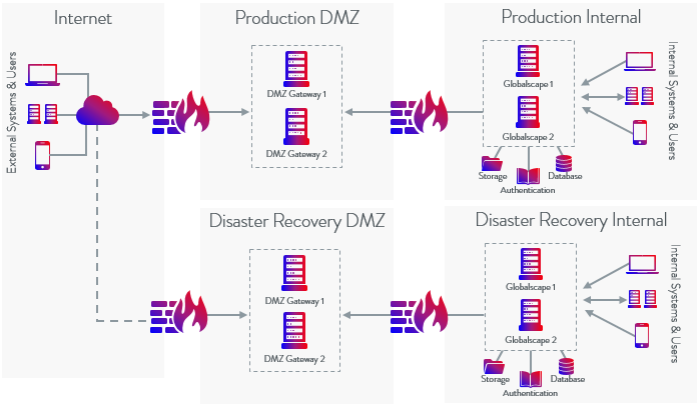
Cluster Type	Supported?
Traditional Active-Active cluster in same LAN	Yes
Primary and DR Site Active-Active cluster (configuration kept mostly in sync)	Yes
Active-Active cluster deployed in the cloud as a static cluster; Support with Windows tools and guidance, but no support on cloud infrastructure or services	Yes
Active-Passive cluster using Microsoft Clustering Services	Yes
Active-Passive cluster using unicast or multicast; Requires email confirmation from customer to account manager that they will be using in failover capacity only	Yes
Active-Active cluster deployed in the cloud as a dynamic, autoscaling cluster; General guidance and recommendations, but no active support	No
Distributed Active-Active cluster (GLBS or Geocluster)	No

HA FAQ

EFT can be configured in an active-active cluster configuration, known as EFT High Availability (HA). In an HA deployment, two or more EFT installations can be configured in an active-active cluster with a shared configuration. EFT acts as its own cluster manager and requires a network load balancer (NLB) to distribute incoming protocol traffic. EFT HA nodes process file transfers at the network level as the NLB directs traffic to it, and can process Folder Monitor and Timer Event Rules in a round-robin fashion (that is, executing the event actions on the first node, then the second, and so on until it comes back to the first node in the list). An example 3-node deployment is shown below. Having at least 3 nodes allows you to take down one node for maintenance and still have 2 active nodes for HA.



You can also install EFT HA in a DR environment:



For best results, before beginning an HA installation, please review all of the information below and refer to the references linked.

Consider the facts below before creating an HA cluster

Installation:

- To install EFT as part of a high availability (HA) cluster, refer to Active-Active HA Cluster--Installing or Upgrading the Server.
- Copy the \web\ folder from the EFT installation folder to the cluster share (%ClusterShare%)
- For true business continuity, you should have **a minimum of three nodes**, so that when one server goes down, nodes on other servers continue to process transactions in high availability, meeting those stringent up-time requirements.
- When EFT is running in HA mode and sharing a network resource, you must run the EFT server service with a Log On account that can access that shared network resource.
- Nodes should be brought online one at a time to avoid getting the nodes out of sync. A node can get out of sync if 1) on administrator login, if the configuration in memory does not match the configuration file on the shared drive; or 2) when the node fails to receive a configuration change message. In either case, the EFT server service will restart and load the latest configuration.
- You can configure additional Sites on non-HA nodes with other authentication to cooperate with the HA-clustered Sites. For example, you could use an AD-authenticated Site on a non-HA node for domain user uploads and downloads, but use the Globalscape, AD, or LDAP-authenticated Sites in the HA cluster for load balancing Event Rules that take place on the files transferred. The non-clustered AD Site would transfer files using the HA shared configuration path as the Site root folder or using virtual folders, while the Event Rule Actions take place on the files on the HA Site.
- If you are using DMZ Gateway®, each EFT must have its own DMZ Gateway; the DMZ Gateway cannot be shared among nodes.
- HA nodes must listen on all IP addresses, rather than each listening on a specific IP address. Do not change the Listening IP address for an HA node. A registry value can be configured to have a different IP address for each node. Refer to Knowledgebase article #11225 for details.
- The default EFT options for DoS/Flood Protection and Login Security settings are designed for each IP to have a single user's activity. These settings can cause EFT to ban the load balancer's IP or intermittently block its activity when all user connections are using the load balancer's IP. **These settings should be disabled when using a load balancer.** It's also a good idea to set an IP access rule to allow the load balancer IP on EFT just in case the settings are accidentally enabled later.

- To make an HA node a stand-alone server, you must uninstall EFT and then reinstall as a stand-alone server. Please contact Sales, Support, or Professional Services for assistance in migrating any existing non-HA deployments to a corresponding HA configuration.
- (In v8.0.5 and later) A stand-alone server can be converted to an HA node. Refer to Promote Stand-Alone EFT to HA node for instructions.
- On HA installations, the EFT server service is configured to restart upon failure on the **Recovery**tab of the service's properties. (Non-HA installations are configured to "take no action" upon failure.)
- You cannot backup in standby and restore in HA or vice versa. You can run restore on any node in the HA cluster. You can restore shared data, node-specific data (listening IP address, DMZ Gateway settings, registration) or both. When the restore process begins, other nodes stop with -1 error. This triggers them to be restarted by Windows Service Manager, at which point those other nodes will wait for restore operation to complete. Once the restore has completed on one of the nodes, the other nodes that had been waiting will proceed with loading configuration. After the restore completes, the node that did restore also restarts in the same way. Thus, all nodes in the cluster have restarted with restored configuration up and running.
- HA Shares should NOT reside on a Unix Samba share. EFT HA environments have a difficult time recovering from network failures that occur on the master node's system.
- (In EFT v8.x and later) The log naming convention now allows for to store logs on the cluster shared drive.

Configuration:

- If using SAML (Web SSO) in an HA environment, SAML needs to have the IDP's public key saved in the HA shared drive.
- After installation, the shared path (for example, \\myserver\HA_config) is shown on the Server's **High Availability**tab > **Config Path**. The shared configuration file PATH cannot be changed in the administration interface. KB #11260 describes how to change the path in the registry.
- On an HA-clustered Site, the **Usr**folder (for example, **\inetpub\EFTRoot\mySite\Usr**), which contains the users' folders, is stored in the shared configuration path.
  (for example, **\\x.x.x.x\inetpub\EFTRoot\mySite\Usr\username**)
  - When using Encrypted folders, you can only encrypt files in the directory hierarchy of the Site's root folder. Make sure that the Site root folder on the **Site > General**tab is pointing to the correct path. That is, if your HA

config drive is on **D:\HAConfig\,**you should edit the site root folder to point to **D:\HAConfig\InetPub\EFTRoot\MySite**.

- When creating an LDAP Site on an HA node, the **User list refresh interval** setting is disabled. The user list must be synchronized on all nodes at the same time.
- A local configuration path for each node must also be specified for each node for local caching. When configuration changes are made to SSH, trusted SSL certificates, OpenPGP key materials, and AML files (Advanced Workflow module workflows), those files are cached locally, and uploads are safely synchronized to the shared config path. The other nodes then update their local cache from the central location. Thus, the central share always contains the current version of those files. When, for example, a new SSL Cert or AML file is created, the creator directly adds/modifies the files on the network share then tells the other nodes that the file was modified/created and they need to update their local cache (that is, copy the file to their local ProgramData directory).
- When using HA, **you need to specify a unique location (local) for the log files**. This is for troubleshooting purposes (to know on which node the issue occurred). Also, having two nodes write to the same file causes issues with file locking, which will cause data in the logs to be lost. For visibility into node status, enable cluster logging. Logging.cfghas new logging options specifically for HA. When configuring RSA in an HA environment be sure to have the **sdconf.rec**file stored locally for each node. Each node MUST have its own copy of sdconf.rec.

MSMQ or Unicast:

- Proper communication among nodes requires:
  - Network adapters on all HA nodes that enable Reliable Multicast Protocol (for the adapters that provide the route between EFT HA nodes)
  - All nodes must be able to send and receive multicast messages, which requires they been on the same LAN subnet
  - L2 Switch between physical computers that host an EFT HA node (physically or virtually) must enable traffic on the LAN segment between HA nodes. Typically, this means enabling IGMP Snoop and IGMP Querier; however, complex deployments (including VPN or MPLS networks between nodes) might require packet encapsulation, such as GRE, to allow packets to operate properly between nodes.
  - Firewalls between HA nodes, and on the computers hosting EFT, must allow the traffic (both multicast and unicast) to pass in and out of the computers. (Windows Firewall will automatically enable the proper ports

when enabling MSMQ.). For physical switches, be sure there are no packet filtering rules that prevent packets of type 113 to flow between nodes.

- If you do not want to use unicast or multicast on your network, you should create a new VLAN for EFT communications. Refer to Knowledgebase articles #11221 and #11276for more information about MSMQ, VLAN, and EFT.

- HA mode of operation for supports IPv6 addressing for inbound and outbound connections. The message queue addressing of nodes within the cluster is not supported on IPv6 addresses. Message queue addressing uses NetBIOS names, not IP addresses, and could be tied to IPv4 on the local LAN subnet that all nodes share.
- When configuration changes are made to SSH, trusted SSL certificates, OpenPGP key materials, and AML files (Advanced Workflow Engine workflows), those files are cached locally, then safely synchronized to the network share. The other nodes then update their local cache from the central location. Thus, the central share always contains the current version of those files.

Event Rules:

- Folder Sweep and archive should be enabled on load balanced Folder Monitor rules to clean up and notify on any events that occur when the primary Event Rule monitor goes down. It is possible to lose some events between when the primary goes down and the next node takes over.
- The "Run On One of" feature in Event Rules currently only supports computer (NetBIOS) names. Refer to Event Rule Load Balancing for more information about the "Run On One of" feature.
- Do not start or provision a new node immediately after making changes to the Event Rule configuration. Give the system at least 30 seconds to process and synchronize the configuration changes.
- When operating in HA mode, the Timer and Folder Monitor Event Rules will execute on ALL of the nodes of the cluster unless you specify at least one High Availability node on which to operate. **Define a default node** for load balancing, as described in High Availability Tab of a Server.
- Because all of the nodes fire **User Account Created** events, each node also runs all **User Account Created** event rules. Therefore, to avoid sending multiple email notifications (for example), you should add an "**If node name**" Condition to the rule so that only one node sends the notification (or performs other Actions).
- In every HA cluster, there will be a "Master" node that performs the Event Rule load balancing assignments.

- Any node may be master; if a master node goes offline, another node will take over as master. Whichever node declares master first becomes master. A node doesn't take over as master until at least one load-balanced Event Rule exists on the system. Prior to a load-balanced Event Rule's existence, all nodes will claim to be master. A master can go down if, for example, MSMQ is stopped, or the network can no longer communicate with the master or the EFT server service for some reason goes down.
- Every 10 seconds each node broadcasts a heartbeat to communicate that they are alive and online. This serves two purposes: 1) Notifies that the master node is up, if the master goes down, then a new node will resume master responsibilities and broadcast that they are now master; 2) Notifies the cluster that the node is online and should be included to handle load-balanced Event Rules.

Auditing and Reporting:

- The ARMreports identify nodes based on computer name. If the node's computer name changes, ARM will see it as a new node and not associate it with the old computer name. (ARM installs an additional set of reports in a "High Availability" folder. These reports are a duplicate of the existing reports, except they report based on Node name.)

COM API:

- The COM API was updated to include HA-specific calls.
- Only one node at a time is allowed to use the administration interface or COM connection. That is, you cannot administer more than one node at a time. (However, more than one administrator can administer the SAME node at the same time, just as in non-HA configurations.) Attempts to administer more than one HA node at a time will prompt an error on nodes other than the first.

Non-High Availability mode vs. High Availability mode EFT

Function	Non-High Availability mode	High Availability mode
Startup	Searches for configuration, tries backup files to handle broken configuration, etc. Always creates "clean" configuration if none is loaded.	Loads only the configuration files from the shared location. *Creates "clean" configuration only if no configuration present. Fails to start if cannot load configuration.*
Shutdown	Updated configuration with latest settings	Does not update configuration.

Function	Non-High Availability mode	High Availability mode
Authentication managers	GS, NTAD, ODBC, LDAP	Globalscape, NTAD, and LDAP
User database refresh	Allowed	Not allowed
PCI cleanup (administrator/user remove/disable for inactivity and send Password Expiration Notifications)	Nightly timer + Every time server deals with user/administrator (user/administrator connection, exposing user/administrator to GUI/COM etc.)	Nightly timer
Client Expiration	Every time when server deals with user (user connection, exposing user to GUI/COM etc.)	Nightly timer
Turning off Autosave and using "ApplyChanges" via COM	Allowed	Not allowed
GUI/COM connection	Always allowed	Only one node at a time is allowed to serve GUI/COM connection
Saving changes made by administrator to FTP.CFG	Background task accumulating changes and saving settings	Only one node can be administered at a time. As soon as you log off of the node on which you've made changes and then log on to second node, those changes would be updated on the second node.
Server restore from backup	Allowed	Allowed
Trial state	Registry	Registry
OTP passwords for clients	Allowed	Not allowed
Legacy password hashes	Allowed	Not allowed
User lock state	Continues after service restart	Breaks after service restart
Invalid login history	Continues after service restart	Resets on service restart

Related Topics

- High Availability Tab of a Server
- Event Rule Load Balancing
- High Availability Message Queuing
- High Availability Tab of a Server
- HA-Related Knowledgebase Articles

Non-High Availability Mode vs. High Availability Mode

Function	Non-High Availability mode	High Availability mode
Startup	Searches for configuration, tries backup files to handle broken configuration, etc. Always creates "clean" configuration if none is loaded.	Loads only the configuration files from the shared location. *Creates "clean" configuration only if no configuration present. Fails to start if cannot load configuration.*
Shutdown	Updated configuration with latest settings	Does not update configuration.
Authentication managers	GS, NTAD, ODBC, LDAP	Globalscape, NTAD, and LDAP
User database refresh	Allowed	Not allowed
PCI cleanup (administrator/ user remove/ disable for inactivity and send password expiration notifications)	Nightly timer + Every time server deals with user/administrator (user/administrator connection, exposing user/administrator to GUI/COM etc.)	Nightly timer
Client Expiration	Every time when server deals with user (user connection, exposing user to GUI/COM etc.)	Nightly timer
Turning off Autosave and using "ApplyChanges" via COM	Allowed	Not allowed
GUI/COM connection	Always allowed	Only one node at a time is allowed to serve GUI/COM connection
Saving changes made by administrator to FTP.CFG	Background task accumulating changes and saving settings	Only one node can be administered at a time. As soon as you log off of the node on which you've made changes and then log on to second node, those changes would be updated on the second node.
Server restore from backup	Allowed	Allowed

Function	Non-High Availability mode	High Availability mode
Trial state	Registry	Registry
OTP passwords for clients	Allowed	Not allowed
Legacy password hashes	Allowed	Not allowed
User lock state	Continues after service restart	Breaks after service restart
Invalid login history	Continues after service restart	Resets on service restart

Active-Active HA Cluster—Installing or Upgrading the Server

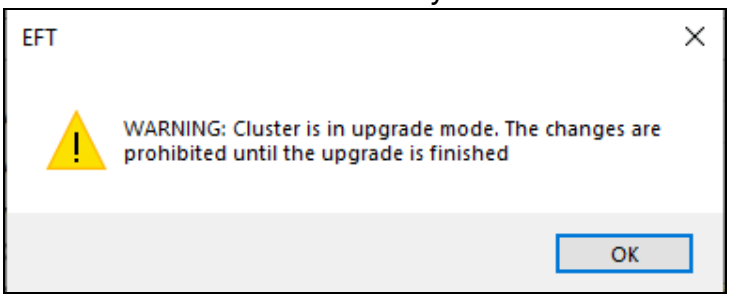
Refer to the Globalscape Knowledgebase article #11271for information about installing or upgrading the server in an active-active, high availability (HA) configuration.

See also Upgrade HA Nodes with Zero Downtime.

Upgrade HA Nodes with Zero Downtime

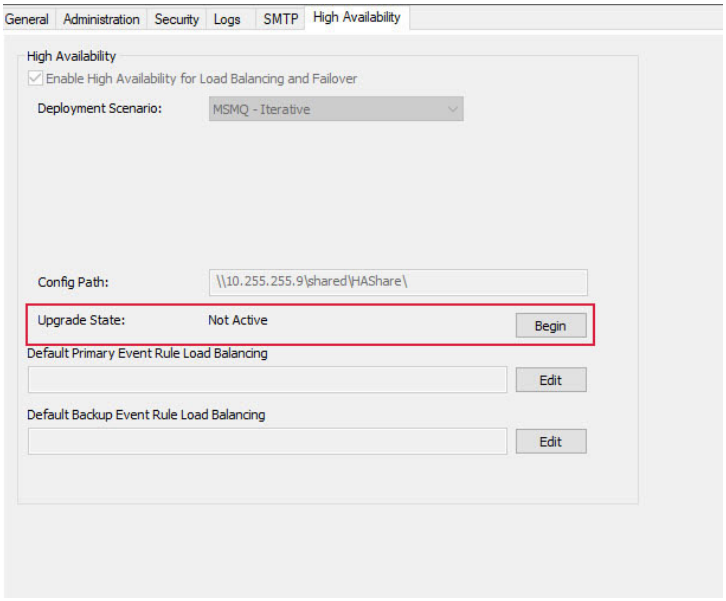
EFT administrators can upgrade their HA nodes with "zero downtime," meaning you can upgrade a cluster without stopping all nodes at the same time.

NOTE: The warning prompt "Cluster is in upgrade mode" is thrown when a user makes a configuration change and then refreshes the EFT administration interface while the server is in "read only" mode.



The Server > HA tab is used to manage the cluster upgrade state

- The button will be displayed as **Begin** when upgrades have not been started.



- The button will be displayed as **End** when upgrades have been completed. Administrators can execute the End state at any point, but nodes that have not been upgraded will fail to start until they are upgraded.
- When enabling the upgrade, EFT administrators will be prompted with a warning

that the transition and change cannot be undone.

- The warning prompt should reference details to review documentation.

To upgrade all of the HA nodes at that same time—without stopping any nodes

In the EFT administration interface, on the **Server > High Availability** tab, you must manually put the cluster into the **Upgrade** state, upgrade each node one by one, then after the upgrade has completed successfully, manually transition the cluster back to **Normal** state.

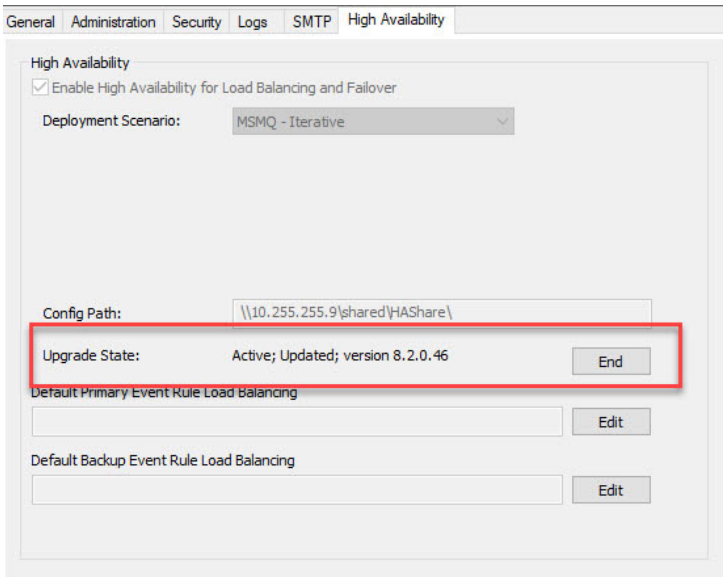
- **Upgrade State**. Allows simultaneous updates to nodes that have an **Outdated** version.

  Upgrade state limitations:

  - Backup/Restore feature is prohibited
  - No configuration changes are allowed during the Upgrade state, except moving the cluster back into the Normal state
- **Normal State**. Requires all nodes have the same version. Upon transition to Normal, the Upgrade State will display “Not Active”

  Normal state limitations:

  - Loading old nodes is prohibited. EFT will not start when the nodes are not upgraded.
  - You will be unable to transition from Upgrade to Normal when an upgrade has not been completed. This only affects nodes that have not been upgraded.
  - EFT will prevent COM API from transitioning from Upgrade to Normal state. A proper response code/error will be presented
  - EFT will prevent REST API from transitioning EFT from Upgrade to Normal state. A proper response code/error will be presented.
  - When upgrade has ended (at the global level or a node that was upgraded), for any nodes that were not upgraded, the EFT Server Service will stop and fail to start until they are upgraded.
  - Transition state from Upgrade to Normal are global, which affects all nodes within the cluster, so administrators should only end upgrades after all nodes have been upgraded.



Upon successful HA upgrade to a new version, the **High Availability** tab's **Upgrade State** will display “Active; Updated; x.x.x.x”, where x.x.x.x is the newer version of EFT (the version to which EFT was upgraded).

Normal state to Upgrade state

- All nodes are Outdated. Admin logins to any of the nodes and enter the cluster into the "Upgrade" state (with GUI/COM/REST).
    - EFT admins shall be able to transition from Normal to the Upgrade state via our EFT administrator interface High Availability tab.
    - EFT admins shall be able to transition from Normal to the Upgrade state via COM. Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade.
    - EFT admins shall be able to transition from Normal to the Upgrade state via REST API. Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade.
    - The ability to start the Upgrade state is a global setting; once set at any node, all nodes will report the same state.
    - Upgrade state should be used ONLY when upgrading to a new version of EFT and not when an EFT administrator forgets to upgrade a node in the cluster from a previous upgrade.
- Once configured for Upgrade, the cluster is in Upgrade state, and you can upgrade each node one by one.

- Outdated nodes write audit data to local *.sql files only; Each node will have their own local *.sql file.
- Updated nodes write into ARM database; If no SQL schema changes exist, there is a post process in the Normal state that will migrate the data from the *.sql file into the ARM database.
- Uses Web folder appropriate to node's version.
    - The nodes' version should match the same version.
    - Shadowfax folder will be copied from \\<HASharedPath>\Web to \\<HASharedPath>\UpgradeFromx.x.xx (where x.x.x.x is the older EFT version); This …\UpgradeFromx.x.x.x will be used for Outdated nodes.
    - Shadowfax folder \\<HASharedPath>\Web will be used for Updated nodes and will be updated with the first upgraded node.
- Outdated nodes allow admins to login in read-only mode. EFT administrators will not be able to make any configuration changes to EFT.
- Updated nodes allow admins to login in read-only mode AND move the cluster to Normal state.
- Configuration changes write in deltas only (there could be only internode mx messages).
    - Changes are not saved into the configuration files, ServerConfig.db and SiteConfigXX.db files. (Part of the advanced property HAFullConfigDumpIntervalMins.)
    - Internode mx messages are communications between EFT nodes (no QA validation).
- Unknown internode messages are ignored; These are internal nodes for Outdated nodes that may not know about freshly added internode messages in Updated nodes.
- Cluster Management subsystem doesn't send any messages and ignores all received messages.
- ERLB subsystem doesn't delegate to run any event rules - all rules are processed with Master node only. Client connections to the server will be processed without any restrictions during the Upgrade state.

Upgrade state to Normal state

- All nodes are Updated. Admin will need to log into any node and end the upgrade which will switch it back to Normal state (with GUI/COM/REST)

    - EFT admins shall be able to transition from Upgrade to Normal state via our EFT Admin UI
    - EFT admins shall be able to transition from Upgrade to Normal state via COM; Appropriate error message(s) will be provided if enabling Normal state on any node when the cluster is already configured for Normal
    - EFT admins shall be able to transition from Upgrade to Normal state via REST API; Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade
    - The ability to end the upgrade state is a global setting; once set at any node, all nodes will report the same state. Nodes that were not upgraded and the upgrade state has ended, will fail to start.
    - Nodes that were not upgraded after the Upgrade state ends, now Normal, can be upgraded later and will be visible and continue to work in the cluster
- Normal state limitations: Loading old nodes is prohibited. EFT will not start when the nodes are not upgraded

COM has several methods to manage cluster upgrade state

- Enum: HAUpgradeNodeState
    - NotInUpgrade = 0,
    - OldNode,
    - NewNode
- Method: ICIServer::GetHAUpgradeNodeState; Retrieves node upgrade state
- REST has two endpoints to manage cluster upgrade state:
    - Get HA node upgrade state; GET /server/ha/upgrade
    - Changes entire HA cluster state to the upgrade or normal state: POST /server/ha/upgrade

Related Topics

- Active-Active HA Cluster Installing or Upgrading the Server
- HA FAQ
- High Availability Tab of a Server

High Availability-Related COM API Objects

Go to the COM API help online to the HA-related COM API objects.

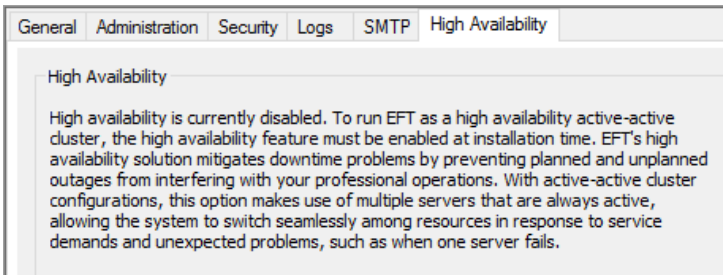
- ICIHighAvailabilityParams
- ICIRoundRobinEventRuleSchedulingParams Interface
- There are other HA-related settings in the ICIServer Interface, ICIEventRule Interface, and enums.
- In the ICIServer Interface:
  - DrainServer
  - GetHighAvailabilityParams
  - HACoherenceQueue
  - HAConfigurationBackupNodeList
  - HAConfigurationDefaultNodeList
  - HAConfigurationFilePath
  - HAEnabled
  - HAEventQueue
  - HAMulticastAddress
  - HAMulticastPort
- In the ICIEventRule Interface:
  - GetHASchedulingParams and SetHASchedulingParams

High Availability Tab of a Server

The **High Availability** tab of the Server is a read-only tab that displays the configuration for high availability (active-active) clustering of EFT. The tab contains the multicast address, port, and listening queues, as well as the default paths for load balancing.

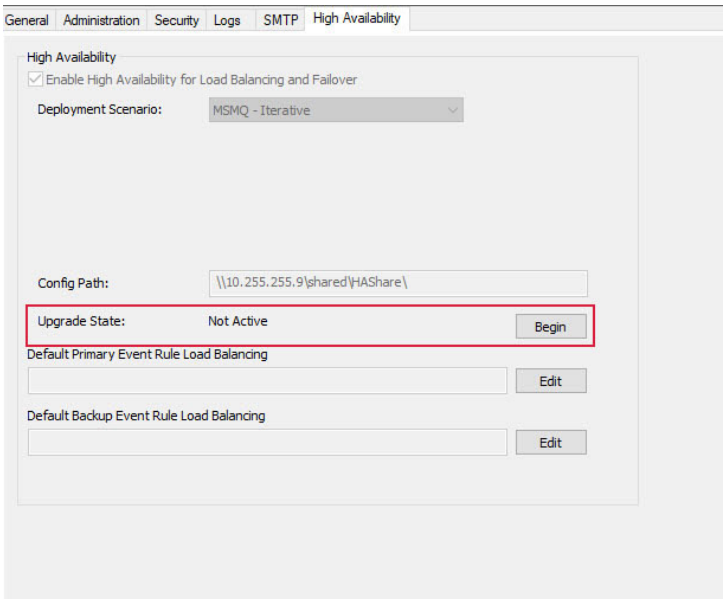
Stand-Alone Server:

If HA is disabled, a message appears explaining that HA is disabled.



HA Server:

If EFT is installed as an active-active or active-passive cluster, the fields below will be displayed.



Deployment Scenario—Displays either MSMQ or Unicast

Multicast Address—The address for the group of nodes in the cluster.

Multicast Port—The port used by the multicast address.

Coherence Queue—Repository for the message queuing (MSMQ) cache that broadcasts messages across the HA cluster to keep all nodes in sync.

Event Queue—Repository where events are held prior to processing.

Config Path—Path at which the cluster's shared configuration is stored.

Upgrade State—If you are upgrading the cluster, click **Begin** to put EFT in read-only mode to begin the upgrade process. The button will display **End** when the upgrade has completed. During upgrade, Upgrade State will display “Active; Outdated; x.x.x.x”, where x.x.x.x is the current EFT version.

Default Primary Event Rule Load Balancing—Here you can click **Edit** to specify the primary node(s) to run load balanced Event Rules.

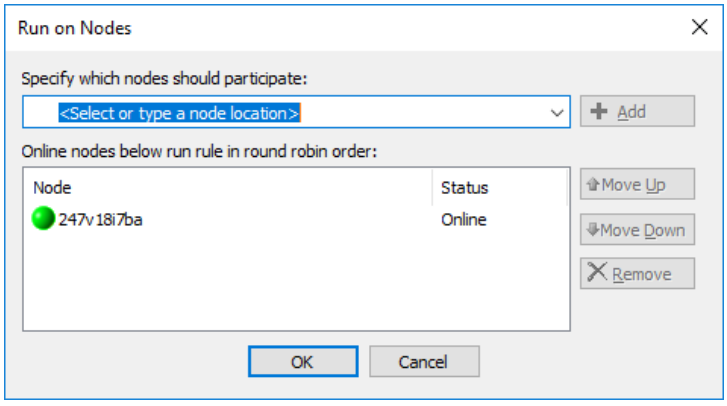
Default Backup Event Rule Load Balancing—Here you can click **Edit** to specify the backup node(s) to run load balanced Event Rules.

- Event Rules will use these default node lists. If the default node list is empty, the Event Rule will execute on ALL nodes of the cluster unless you explicitly specify which node is to run the Event Rule when you define the Event Rule.

To define the default Event Rule load balancing nodes

1. In the administration interface, connect to EFT and click the **Server** tab.
2. Click the **High Availability**tab.

   Next to the **Default Primary Event Rule Load Balancing** and **Default Backup Event Rule Load Balancing**, click **Edit**. The **Run on Nodes** dialog box appears.



3. Click the down arrow to select a node, click **Add**, then click **OK**.

Related Topics

- High Availability Overview
- HA FAQ
- Server Drain, Maintenance, and Auto-Restart
- Unicast
- High Availability Message Queuing
- Active-Active HA Cluster—Installing or Upgrading the Server
- Upgrade an HA Cluster with Zero Downtime
- HA-Related Knowledgebase Articles
- Event Rule Load Balancing

High Availability Message Queuing

EFT High Availability (HA) installations for active-active clustering can use Microsoft Message Queuing (MSMQ) to share configuration and other data among nodes. All MSMQ messages are two-fish encrypted. MSMQ Broadcasting is used to communicate that a change has been made to the cluster. When an administrator makes a change to the configuration (adds/disables a user, creates an event rule, etc.), the node will broadcast a message to all nodes in the cluster that the configuration file has been modified, and to read in the changes. The broadcasting system is also used to notify other nodes when AML, SSL, SSH, and OpenPGP files are created or modified.

Almost all EFT data and operations are synced between all of the nodes, except for the following node-specific data/operations:

- Trial state
- DMZ Gateway settings
- Pending certificates
- Site Start/Stop
- Temporary user lockout
- Invalid login attempts history (when the limit is reached the user is disabled cluster-wide)
- Temporary IP ban (permanent ban is cluster-wide)
- File Lock (hiding the files being uploaded from other connections)

When EFT is installed for active-active clustering, the installer determines whether MSMQ is enabled, and enables it if it is not. EFT HA relies on the MSMQ service for two important functions:

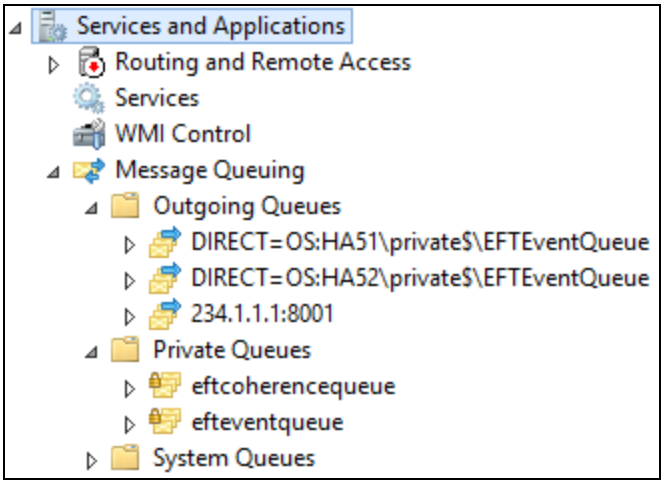
- Synchronize changes made to the cluster configuration (eftcoherencequeue)
- Load balance Event Rules (efteventqueue)

The Event queue and the Coherence queue are created at service start and destroyed when the service is stopped. They appear in the Computer Management console, under **Services and Applications > Message Queuing**.

To view Message Queuing

1. Right-click the **Start**icon, then click **Run**.
2. In the **Run**dialog box, type `compmgmt.msc` then press ENTER.
3. Expand the **Services and Applications** node.

4. Expand the **Message Queuing** node.

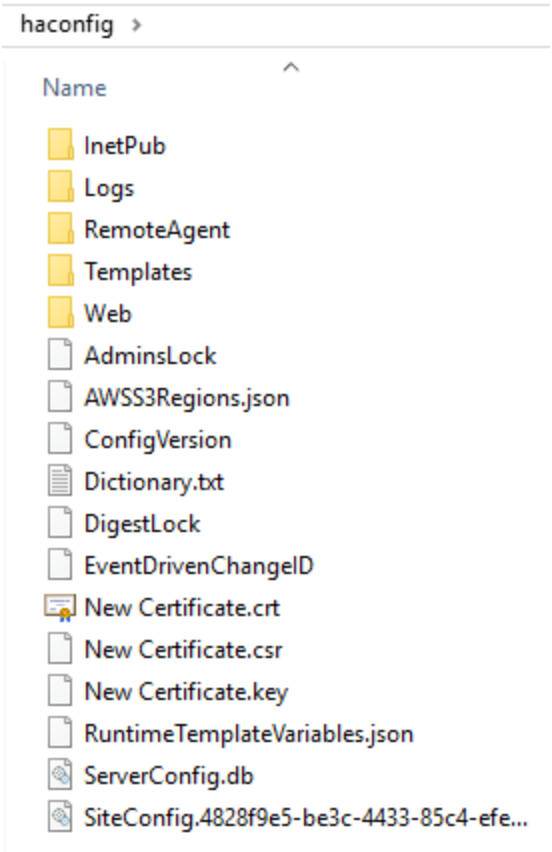


Related Topics

- EFT HA (Active-Active) Deployment
- Unicast
- Event Rule Load Balancing
- High Availability Tab of a Server

HA Nodes Configuration Files

When installing EFT in an HA configuration, you must specify a shared configuration location (which must be accessible by all of the nodes in the HA cluster). The files that all of the HA nodes will share are saved and updated in the shared configuration directory.



- An Advanced Property was added to improve performance when configuration is copied to the cluster share. When off, `HAFullConfigDumpIntervalMins = 0` or is not defined, the full configuration is copied on each change. Add the Advanced Property and set it between 1-10 minute intervals to reduce network traffic.
- A local configuration path for each node must also be specified for each node for local caching. When configuration changes are made to SSH, trusted SSL certificates, OpenPGP key materials, and AML files (Advanced Workflow tasks), those files are cached locally, and uploads are safely synchronized to the shared config path.

The other nodes then update their local cache from the central location. Thus, the central share always contains the current version of those files. When, for example, a new SSL Cert or AML file is created, the creator directly adds/modifies the files on the network share then tells the other nodes that the file was modified/created and they need to update their local cache (that is, copy the file to their local ProgramData directory).

- When using HA, **you need to specify a unique location (local) for the log files**. This is for troubleshooting purposes (to know on which node the issue occurred). Also, having two nodes write to the same file causes issues with file locking, which will cause data in the logs to be lost. For visibility into node status, enable cluster logging. Logging.cfghas new logging options specifically for HA. When configuring RSA in an HA environment be sure to have the **sdconf.rec**file stored locally for each node. Each node MUST have its own copy of sdconf.rec.
- When using Encrypted folders, you can only encrypt files in the directory hierarchy of the Site's root folder. Make sure that the Site root folder on the **Site > General** tab is pointing to the correct path. That is, if your HA config drive is on **D:\HAConfig\,** you should edit the site root folder to point to **D:\HAConfig\InetPub\EFTRoot\MySite**.

Related Topics

- Logging for HA Nodes
- HA FAQ

Node Discovery Using Shared Storage for HA Clusters

The EFT HA Resiliency project replaces MSMQ UDP Multicast with iterative MSMQ TCP Unicast (that is, message is sent to each the nodes individually over MSMQ TCP). In addition to the improved reliability of TCP, removing the dependence of UDP Multicast simplifies deployment on cloud infrastructures. However, a new method of discovering of nodes is required, and can be accomplished using the shared storage (with file locking semantics) that EFT already requires.

ActiveNodes.json File

For EFT HA clusters, node discovery is accomplished through an ActiveNodes.json file on the existing shared storage. All access to ActiveNodes.json is performed in exclusive access mode (so no one else changes or reads the file while accessing it). The ActiveNodes.json file is the “one source of truth” for which nodes are connected when operating in any HA mode. To determine where to send the nodes, the ActiveNodes.json must be consulted. Nodes will be responsible for adding and removing themselves from the list. The "Event Rule Master" (that is, the node that is holding the lock on Master.lck) is responsible for periodically removing nodes that failed without removing themselves.

ActiveNodes.json file example:

```
{
 "Nodes": [{
 "Name": "EFT_NODE_1",
 "IP": ["192.168.1.101"],
 "ActivationTime": "2017-03-30T15:20:30-06:00"
},{
"Name": "EFT_NODE_2",
"IP": ["192.168.1.102"],"ActivationTime": "2017-03-30T15:20:35-
06:00"
}]
}
```

Sending “Multicast” Messages

To determine which nodes to send the “Multicast” messages to, ActiveNodes.js is consulted.

1. If ActiveNodes.json has been modified (Check both last modified Date/Time and file size)

2. Open ActiveNodes.json in “OPEN_ALWAYS” and “Exclusive Access” mode (locks file from access by others)
3. Retry up to 10 times, waiting 100ms between each, if file is locked by another process
4. If cannot open the file after all retries, EFT shall write an error to EFT.log and shall indicate that cached values will be used
5. Read file contents
6. Close ActiveNodes.json
7. Parse JSON file contents (optimization, if this is done after the file is closed)
8. Store the cached values for future use
9. Send the message to each node listed in the JSON (or cached value if could not open file)

Node Adding Self

When a node starts up it updates the ActiveNodes.json file, adding itself.

- Open ActiveNodes.json in “OPEN_ALWAYS” and “Exclusive Access” mode (locks file from access by others)
    - Retry up to 300 times, waiting 100ms between each, if file is locked by another process
    - If cannot open the file after all retries, EFT shall write an error to EFT.log and Windows Event Log, and for abject failure leading to restart
    - Service should exit in FAILURE mode
- Read file contents
- Parse JSON file contents
- If this node is not already in list (normally it shouldn’t be, but if current node had failed and restarted it may)
    - Add entry for this node to the JSON
    - Write Updated JSON File Contents (truncating file as needed)
- Close ActiveNodes.json
- Store the cached values for future use

Node Removing Self

When a node shuts down it updates the ActiveNodes.json file, removing itself.

- Open ActiveNodes.json in “OPEN_ALWAYS” and “Exclusive Access” mode (locks file from access by others)

        - Read file contents
            - Retry up to 3 times, waiting 100ms between each, if file is locked by another process
            - If cannot open the file after all retries, EFT shall write an error to EFT.log and Windows Event Log
    - Parse JSON file contents
    - If this node is in list (it should be)
        - Remove entry for this node
        - Write Updated JSON File Contents (truncating file as needed)
    - Close ActiveNodes.json

Event Rule Master Removing "Expired" Nodes

Periodically the Event Rule Master updates the ActiveNodes.js file, removing any expired nodes.

- Open ActiveNodes.json in "OPEN_ALWAYS" and "Exclusive Access" mode (locks file from access by others)
    - Retry up to 4 times, waiting 100ms between each, if file is locked by another process
    - If cannot open the file after all retries, EFT shall write a warning to EFT.log
- Read file contents
- Parse JSON file contents
- Remove expired nodes from list, (i.e. all of the following conditions are met)
- Use the "decay" mechanism in EFT (2x missed heartbeat from a node means the node is down)
- If any nodes removed, write Updated JSON File Contents (truncating file as needed)
- Close ActiveNodes.json

EFT System Architecture

EFT can be installed as a stand-alone deployment with one server (which can have multiple Sites/IP addresses). Several more complex options are available for how you configure EFT in your network architecture, described below, depending on what you need to accomplish.

Refer to the EFT System Architecture Guide in the Knowledgebase for descriptions and illustrations of the various architectures available.

Talk to your account manager or the Globalscape Professional Services team to design a custom architecture.

Server Drain, Maintenance, and Auto-Restart

Draining the server provides for graceful shutdown and transition between EFT and HA nodes. Drain mode halts any NEW incoming connections and HA Event Rule activity for all Sites on a specific node. Transfers and events in progress would continue to operate until completion. When in drain mode, the node relinquishes mastership and the master stops delegating events to the drained node. If a certain node/server is expected to restart (for example, after Windows updates), administrators can preemptively manually drain the node before the expected restart. In this way, all traffic is routed to and kicked off on the other nodes not paused. After the Windows update/maintenance of the node, traffic and event rule activity will resume normally.

Limitations

- The WTC will deny uploads for any pending transfers on nodes that are in drain mode; in-progress transfers will be permitted to complete (unless drain timeout occurs).
- When EFT enters drain mode, it denies all future connections. scClient may do some GET requests when a file completes upload during drain to obtain a refreshed directory listing. EFT will deny these requests and issue an error. These errors can be ignored; all uploads in progress will continue until completion or until drain timeout occurs.

To enable drain mode manually

1. In the EFT administration interface, click **File > Drain Server** (or use the COM API method, **ICIServer::DrainServer**). A message appears asking if you want to restart the server service after draining.
2. Click **Yes** to automatically restart; click **No** if you want to restart later.

Auto-Drain

Auto-Drain takes effect automatically when an HA node detects that it is out of sync and a restart is required. The server engages Drain mode (waits for transfers and events to complete) and then automatically restarts the node to regain sync with the cluster.

The administrator can configure the time before drain takes effect, and the time it will allow for transfer and processes to complete, and can disable drain completely, if wanted.

Refer to https://kb.globalscape.com/KnowledgebaseArticle11391.aspxfor the overrides pertaining to Server Drain, Maintenance, and Auto-Restart

Unicast

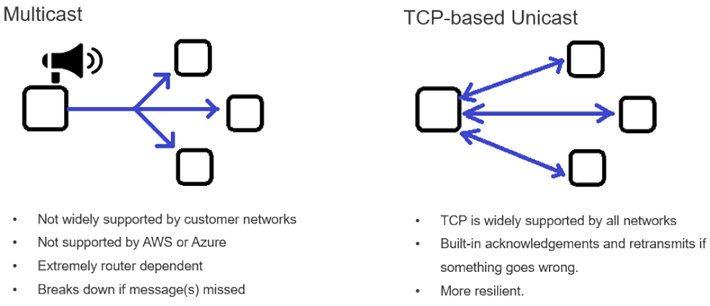
Iterative TCP Unicast (that is, message is sent to each the nodes individually over TCP) can be used instead of MSMQ UDP Multicast. In addition to the improved reliability of TCP, removing the dependence of UDP Multicast simplifies deployment on cloud infrastructures. Discovering of nodes can be accomplished using the shared storage (with file locking semantics) that EFT already requires.

The advanced property below must be enabled to use Unicast:

```
"ClusterCoherenceQueueMsmqType":"msmq-iterative"
```

Unicast provides:

- HA support for environments that do not support MSMQ Broadcasting
- Ability for HA to work in a vMotion environment
- Improved support for node-out-of-sync detection and availability.

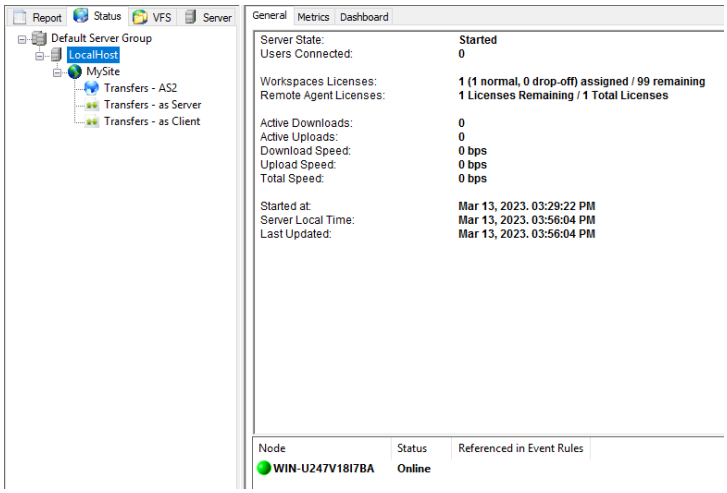


Viewing Server or Node Status

In the administration interface, you can view the status of EFT in real time, such as number of users connected, average speed, and so on. You can view Server status on the **Status** tab or on the Server node's **General**tab.

To view status on the Statustab

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Status**tab, click the **Server** node. EFT's statistics appear in the right pane.



3. In an HA cluster, you can see the nodes and their status at the bottom of the **Status**viewer.
    - **Online**: EFT server service is up and communicating via Heartbeat to the rest of the node in the cluster
    - **Master**: Same status as **Online**, however this node is designated as the **Master**node for Event Rules Load balancing.

Only one node can be show as Master in the list of the nodes from the cluster. This status only is displayed if you have at least one Event Rule enabled and configured to run in more than one node from the cluster. If this status exists, the Master node will create an exclusive file lock onto **MasterNodeLock**file in the HA config shared folder.

- **Offline**: EFT server service is down; no communication via Heartbeat is performed
- **Unknown**: A node name is being reference in at least one Event Rule; however, this node name is not part of the cluster.

To view status on the Server tab

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Server** node.
3. In the right pane, click the **General**tab. EFT's statistics appear in the right pane.
    - **Server status**: Displays "Service is started" or "Service is stopped." You can also stop and start the EFT service on this tab.
    - **Start date/time**: Displays the date and time that the EFT service was last started.
    - **Uptime**: Displays the length of time that the EFT service has been running since it was last started.
    - **Last modified time**: Displays the date and time that EFT was last modified.
    - **Last modified by**: Displays the username of the user who last modified EFT.
    - **Active sessions**: Displays the number of users who are currently logged in to EFT.
    - **Active uploads**: Displays the number of uploads in progress.
    - **Active downloads**: Displays the number downloads in progress.
    - **Average speed**: Displays the average transfer speed.
    - **Workspaces licenses**: Displays the number of licenses used and number licensed (allowed)
    - **Web clients licenses**: Displays the number of licenses used and number licensed (allowed)

Logging for HA Nodes

The EFT cluster administrator has access to the EFT logs from the shared drive and doesn't have to navigate to the nodes to view them.

On the **Server > Logs** tab, you can specify a shared log location and prefix the log filename with a node ID. However, if you upgrade an HA environment from EFT version 7.4.x or earlier, the **Log File Settings**path is not updated; it keeps the old path where the cluster administrator had to navigate to the different nodes to view the log files. Instead, you can manually provide the shared configuration path with the server node name. (for example, \\ipaddress\share\log\%SERVER.NODE_NAME%\). Once you've changed the Log File Settings path, a folder for each node should appear in the shared path, and new log files will be saved there.

Log files are not backed up in the Backup and Cleanup Rule, because that is intended as a configuration backup. Once you've changed the Log File Settings path, you can create your own Event Rule to back up log files.

HA-Related Knowledgebase Articles

The following Knowledgebase (KB) articles can assist with configuring EFT in an HA environment:

- 11146 - Installing or Upgrading EFT in a Failover, Active-Passive Cluster
- 11175 - Load balanced Folder Monitor events fail to process files in an HA clustered environment
- 11197 - Message appears stating that the node is out of sync and that the service needs to be restarted
- 11214 - Performance Tuning EFT HA Native mode
- 11215 - NetApp NAS tuning to work with EFT in HA mode
- 11216 - How to Mirror an EFT HA (Active-Active) Cluster to another EFT HA (Active-Active) Cluster Manually
- 11221 - EFT HA can Reliable Multicast and MSMQ to communicate between nodes
- 11224 - Inbound F5 Load Balancing for an EFT HA Cluster using DMZ Gateways
- 11225 - Node-specific IP address on HA site
- 11245 - Folder Monitors and Shared Storage
- 11260 - Changing the path to the shared configuration folder for EFT with HA
- 11271 - Installing and Upgrading EFT in an Active-Active HA Cluster
- 11276 - Integrating EFT HA in a network with a Cisco switch
- 11269 - EFT banning load balancer IP address
- 11302 - Why do clients connect to EFT showing the IP of the Netscaler load balancer?
- 11314 - Load Balancers and IP addresses
- 11391 - Registry settings for HA server drain and coherence
- 11407 - Using SSL/TLS termination at F5 Load Balancer
- 11483 - Unable to set refresh interval on LDAP/AD site when EFT configured in HA
- 11486 - Event rule sending duplicate emails in HA environment for User Account Created event
- 11504 - Cluster-Related Advanced Properties
- 11542 - Promote Stand-Alone EFT to HA node

Configuring SSL

The topics below provide information regarding configuring SSL.

- SSL Overview
- Explicit Versus Implicit SSL
- SSL Certificates
- SSL Encryption Algorithms
- SSL Certificate Compatibility
- TLS 1.3 Support
- Assigning a Certificate
- Certificate Chaining
- Certificate Manager
- Creating SSL Certificates
- Enabling SSL on the Server
- Enabling SSL on the Site
- Configuring SSL for a Settings Template or User Account
- Exporting a Certificate
- Exporting a Certificate from PFX to PEM
- Importing a Certificate
- Signing a Certificate
- SSL Certificate Expiration Notification
- SSL Certificate-Based Login
- Disabling SSL Connections on the Site
- Using OpenSSL to Generate/Convert Keys and Certificates

SSL Overview

Secure Socket Layer (SSL) is a protocol for encrypting and decrypting data across a secure connection from a client to a server with SSL capabilities. EFT is responsible for sending the client a certificate and a public key for encryption. If the client trusts EFT's certificate, an SSL connection can be established. All data passing from one side to the other will be encrypted. Only the client and EFT will be able to decrypt the data.

EFT supports SSL for client and server authentication, message integrity, and confidentiality. You can configure EFT's security features to verify users' identities, allows users to verify your identity, and to encrypt file transfers. The key to understanding how SSL works is to understand the elements that take part in the process.

FTPS is an enhancement to standard FTP that uses standard FTP commands (and protocol) over secure sockets. FTPS adds SSL security in both the protocol and data channels. FTPS is also known as FTP-SSL and FTP-over-SSL. You might also see the term SSL used in conjunction with *TLS*. SSL has been merged with other protocols and authentication methods into a new protocol known as Transport Layer Security (TLS). EFT employs SSL/TLS to perform FTPS to keep your data secure. Refer to EFT Specifications for information about the OpenSSL version used in this version of EFT.

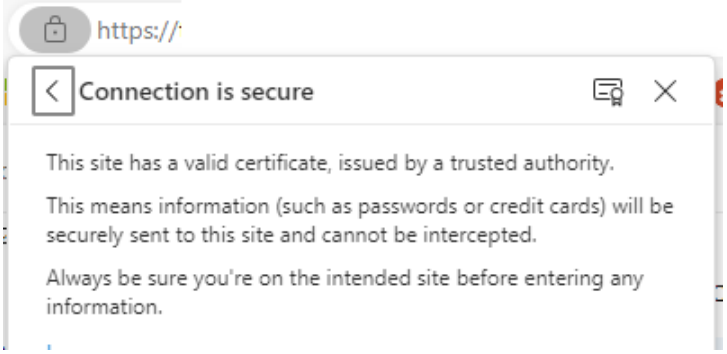
EFT's SSL implementation uses all the SSL configuration made on the **Server** > **Security** tab for all SSL operations, including Event Rules.

Elements that Work Together to Establish a Secure SSL Connection:

- **Client**: The client needs to be an FTP client with SSL capabilities.
- **Certificate**: Certificates are digital identification documents that allow both servers and clients to authenticate each other. Server certificates contain information about your company and the organization that issued the certificate (such as Verisign or Thawte) while client certificates contain information about the user and the organization that signed the certificate. You can choose to either trust or distrust a certificate. In some cases, the client's certificate must be signed by EFT's certificate to open an SSL connection.
- **Session Key**: The client and EFT use the session key to encrypt data. It is created by the client via EFT’s public key.
- **Public Key**: The client encrypts a session key with EFT’s public key. It does not exist as a file, but is produced when a certificate and private key are created.
- **Private Key**: EFT's private key decrypts the client's session. The private key is part of the public-private key pair.

- **Certificate Signing Request**: A Certificate Signing Request (CSR) is an unsigned copy of your certificate. A certificate signing request is generated each time a certificate is created. A certificate signing request has a .csr extension. This file is used when you need to have your certificate signed. Once the .csr file is signed, a new certificate is created and replaces the unsigned certificate.

NOTE: Certain browsers check expiration and other data about the certificate to ensure you have a secure connection. Browsers like Chrome will tell you if you have a valid certificate when you click on the padlock icon next to the URL:



SSL must first be enabled on the Server and Site, and then can be enabled in the Settings Template and/or for each user. EFT provides administrators the ability to specify the symmetric key cipher(s) and the ordering of those ciphers for establishing SSL sessions. EFT validates inbound SSL sessions, and allows or denies connections based on specified or approved ciphers.

EFT supports two levels of authentication with SSL:

- **High** - EFT is configured so that it contains a certificate, but does not require a certificate from the FTP client.
- **Highest** - EFT is configured so that it provides a certificate and also requests a certificate from the client. EFT compares the client certificate to a list contained in its Trusted Certificates database. EFT either accepts or rejects the connection based upon a match.

Related Topics

- FIPS-Certified Library for SSL Connections
- SSL Certificates
- SSL Certificate-Based Login
- SSL Certificate Compatibility
- Enabling SSL on the Server
- Enabling FTPS and HTTPS (SSL) at the Site Level
- Explicit Versus Implicit SSL

- Creating SSL Certificates
- Certificate Chaining
- Assigning a Certificate
- Signing a Certificate
- Certificate Manager
- Importing a Certificate
- Exporting a Certificate
- Disabling SSL Connections
- Exporting a Certificate from PFX to PEM
- Using OpenSSL to Generate/Convert Keys and Certificates

Explicit Versus Implicit SSL

Secure Socket Layer (SSL) was originally created for secure Web browsing. When both a client and server support the AUTH SSL command, security is accomplished through a sequence of commands passed between the two computers. The FTP protocol definition provides at least two distinct mechanisms by which this sequence is initiated: explicit (active) and implicit (passive) security.

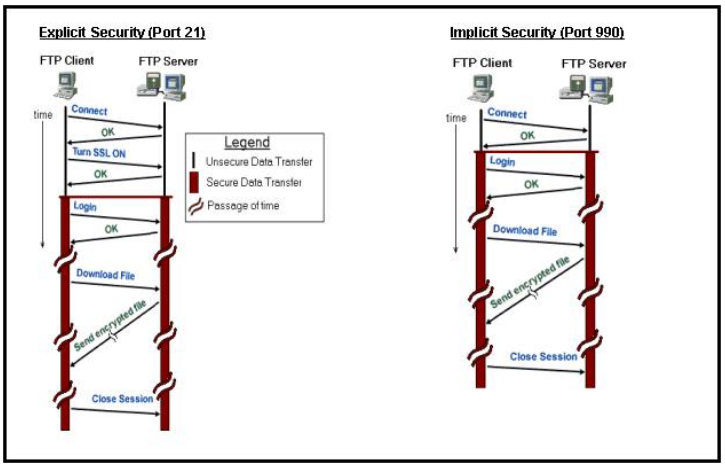
Explicit Security: To establish the SSL link, explicit security requires that the FTP client issue a specific command to the FTP server after establishing a connection. The default FTP server port is used. This formal method is documented in RFC 2228.

Implicit Security: Implicit security automatically begins with an SSL connection as soon as the FTP client connects to an FTP server. In implicit security, the FTP server defines a specific port for the client (990) to be used for secure connections.

Implicit SSL is discussed in various SSL drafts, but is not formally adopted in an RFC. For strict compliance to standards, use the explicit method.

Because implicit SSL has a dedicated port strictly used for secure connections, implicit SSL connections require less overhead when you establish the session. There are various FTP servers that support this mode, including EFT, RaidenFTPD, IBackup's FTP server, and others.

Think of implicit security as "always on" and explicit security as "turn on." The following diagram contrasts implicit and explicit SSL connections.



SSL Certificates

The key to understanding how SSL works is to understand the elements that take part in the process. A key element of SSL is the SSL certificate. A public-key certificate (usually just called a certificate) is a digitally-signed document that ties the value of the public key to the identity of the server service that holds the corresponding private key.

Typically, a certificate contains the following information:

- EFT's public key value, which the clients use to encrypt a session key (the client and EFT use the session key to encrypt data). This public-key does not exist as a file. It is produced when a certificate and private key are created.
- EFT's identifier information, such as the name, email address, common domain name, and other details.
- The validity period (the time that the certificate is considered valid)
- Issuer or signer identifier information
- The digital signature of the issuer, which attests to the validity of the binding between EFT public key and the organization's identifier information.

Many certificate types or standards exist, and EFT supports the most common ones. EFT can import into its certificate store any client-provided certificate of type PKCS 7 or 12, and the X.509 DER encoded standard. For the certificate that EFT itself provides (to the connecting client during the SSL handshake), it supports X.509 and PKCS #12 only. Note that PKCS #12 embeds both the certificate AND private key into a single file. The default type that is created by EFT is x.509 base-64 standard DER encoded.

Before a certificate can be used for securing connections, it must be created (generated) and signed (or vouched for). Certificates can be created directly from EFT, or by a trusted Certificate Authority (CA), which is an independent and trustworthy entity responsible for issuing and managing digital certificates, including revocation of certificates that are expired or are otherwise unauthorized. Once created, a certificate should be signed. By digitally "signing" a newly issued certificate, the signer guarantees the authenticity of the data held in the signee's certificate. EFT can sign its own certificates; however, it is recommended that the certificate be signed by a trusted 3rd-party CA.

When generating a new certificate, EFT creates a self-signed certificate and a certificate signing request (or CSR) file that you can send to a CA for signing and then import into EFT.

Files created by EFT:

- **Private key file (.key)** - The private key should never be distributed to anyone. It is used to decrypt the session that is encrypted by the public key.
- **Certificate request file (.csr)** - Each time you create a certificate using the wizard in EFT, a Certificate request file is also created. This file can be signed by EFT's Certificate Signing Utility or sent to intermediate certificate authority such as GeoTrust, Verisign (www.verisign.com), or Thawte (www.thawte.com) for signing.
- **Certificate file (.crt)** - This is a self-signed certificate. To obtain a 3rd-party signed certificate, you must send the certificate signing request file to a Certificate Authority (CA) such as Verisign, Geotrust, or Thawte. The CA in turn will send you a new **.crt**file with which you can replace your self-signed one.

SSL Certificate Chain-of-Trust

Trust in a certificate is established when you have a copy of the signing certificate in your certificate store (for example, EFT's store or Internet Explorer's Trusted Root Certification Authority for clients). The certificate does not necessarily have to be signed by a root CA; it can be signed by subordinate intermediate CA, as long as there is a valid certification path from the signing certificate to a trusted root certificate, meaning that none of the certificates in the certification path have been revoked or is expired.

Related Topics

- Enabling SSL on the Server
- Remote administration
- Configuring SSL for a Site
- Enabling FTPS, HTTPS (SSL) on a Site
- Explicit Versus Implicit SSL

- SSL Certificates
- SSL Certificate-Based Login
- SSL Certificate Compatibility
- The AS2 Module
- FIPS-Certified Library for SSL Connections
- Creating SSL Certificates
- Certificate Chaining
- Assigning a Certificate
- Signing a Certificate
- Certificate Manager
- Importing a Certificate
- Exporting a Certificate
- Disabling SSL Connections
- Exporting a Certificate from PFX to PEM
- Using OpenSSL to Generate/Convert Keys and Certificates

SSL Encryption Algorithms

The table below lists the SSL encryption algorithms available in EFT and the Advanced Workflow Module (AWM). It is up to you to determine which settings to use in your environment.

SSL/TLS	Protocol Version	Encryption	Message Authentication Code (MAC) – Hashing algorithm	Key Exchange	Authentication	Cipher Suite Version
EFT	• TLSv1.2 • TLSv1.1 • TLSv1.0 • SSLv3	• AESGCM (256) • AES (256) • Camellia (256) • AESGCM (128) • AES (128) • SEED (128) • Camellia (128) • IDEA (128) • RC4 (128) • 3DES (128) • EFT uses the OpenSSL FIPS Object Module	• AHEAD • SHA384 • SHA1 • SHA256 • MD5	• ECDH • DH/DSS • DH • DH/RSA • ECDH/RSA • ECDH/ECDSA • RSA • Key lengths supported: 1024, 2048, 3072, and 4096 bits	• RSA • ECDSA • DH • DSS • None • ECDH	• TLSv1.2 • SSLv3

SSL/TLS	Protocol Version	Encryption	Message Authentication Code (MAC) – Hashing algorithm	Key Exchange	Authentication	Cipher Suite Version
AWM	• TLSv1.2 • TLSv1.1 • TLSv1.0 • SSLv3	• AES (256) - CBC • AES (128) - CBC • RC4 (128) • 3DES (128) – EDE - CBC • RC4 (128) • RC4 (56) • RC4 (40) • RC2 (40) - CBC • DES - CBC • DES (40) - CBC	• SHA256 • SHA1 • MD5	• DH/DSS • DH • DH/RSA • RSA	• RSA • DSS • None	• TLSv1.2 • SSLv3

SSL Certificate Compatibility

The table below indicates the types of functions and associated encoding that have been tested for compatibility on EFT.

EFT does not support SSL Certificate Private Keys without passphrases.

	Encoding			
Function	**PEM - ASCII encoded**	**DER - binary encoded**	**PKCS#7/P7B**	**PKCS#12/PFX**
AS2 public	YES	YES	YES	YES (imports public key)
AS2 private	YES	YES	n/a	YES
AS2 partner public	YES	YES	YES	n/a
General SSL public	YES	YES	YES	YES (imports public key)
General SSL private	YES	YES	n/a	YES
Create Public Certificate	YES	YES	YES	n/a
Create Private Certificate	YES	YES	n/a	YES
Certificate Manager Import	YES	YES	YES	YES (imports public key only)
Certificate Manager Export	YES (public only)	YES (public only)	YES (public only)	n/a

TLS 1.3 Support

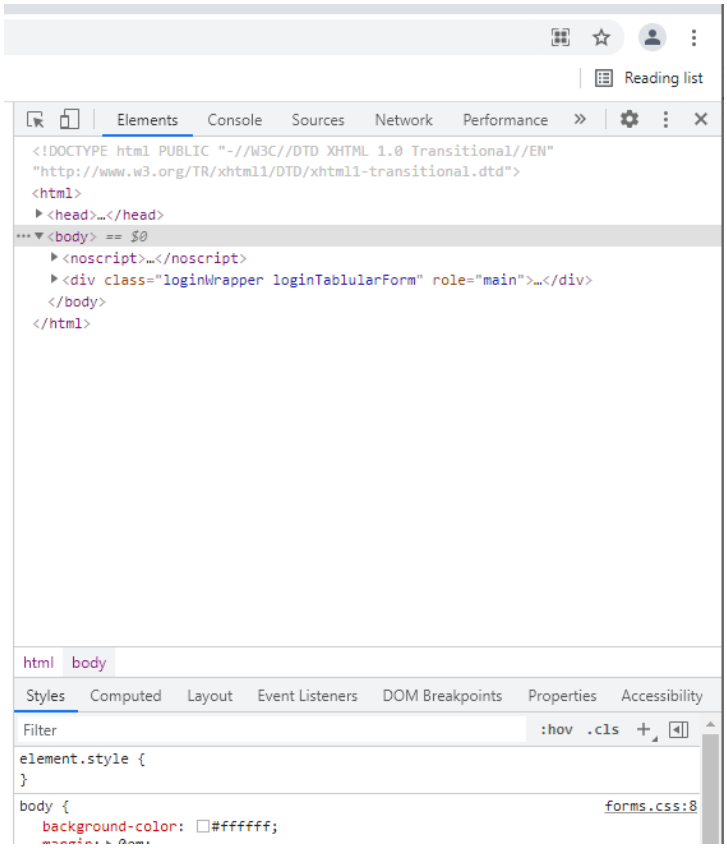
EFT v8.0.6 and later support the TLS 1.3 protocol with OpenSSL v1.1.1.

TLS 1.3 can be selected in the protocol list in the **TLS Settings** dialog box. It is enabled by default. TLS 1.3 can also be disabled/ turned off in favor of using a different variant, such as TLS 1.2. There is no TLS 1.3 available in FIPS mode. (EFT in FIPS mode continues to use v1.0.2u.)

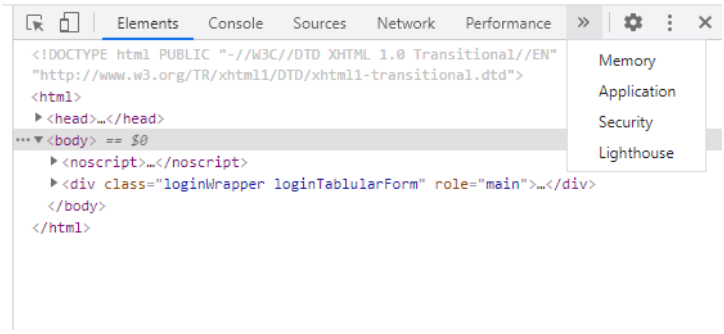
You can use developer tools in the browser to verify that the Web Transfer Client is using TLS.

To verify that TLS 1.3 is being used

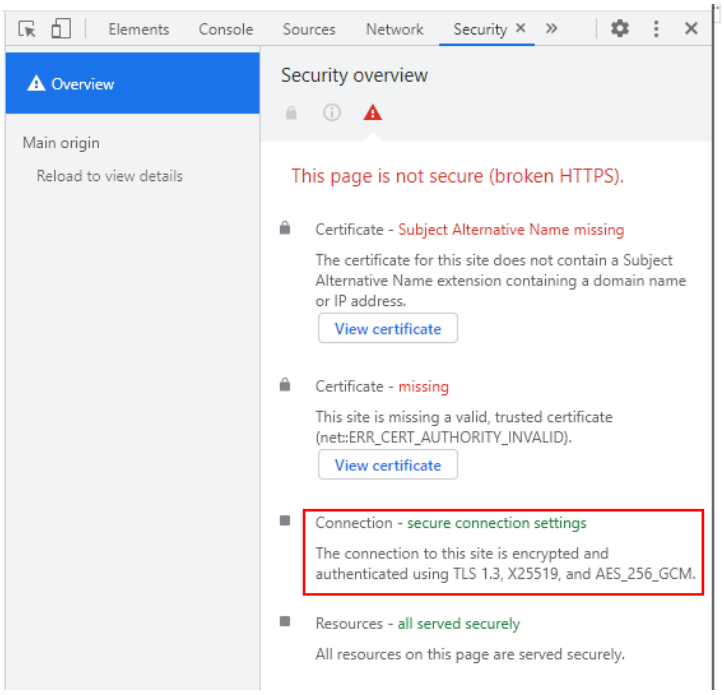
1. Open your browser and navigate to the Web Transfer Client URL, such as https://localhost/Web/Account/Login.htm.
2. Do not log in.
3. Maximize the browser window.
4. Press F12 on your keyboard.



5. Click the right-facing arrows to open the drop-down box:



6. Click **Security**. The **Security overview** appears.



The Connection section describes whether the connection is encrypted and which ciphers are being used. (This screen shot was taken on a test system and did not have a valid certificate. That information is also displayed here on the Security tab.)

The following 25 ciphers are enabled by default:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-CCM8
- ECDHE-ECDSA-AES128-CCM
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- AES128-GCM-SHA256
- AES128-CCM8
- AES128-CCM
- AES128-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-CCM8
- ECDHE-ECDSA-AES256-CCM
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- AES256-GCM-SHA384
- AES256-CCM8
- AES256-CCM
- AES256-SHA256
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305

The following algorithms are only available when FIPS is turned off:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES256-CCM8
- AES256-CCM8
- ECDHE-ECDSA-AES256-CCM
- DHE-RSA-AES256-CCM
- AES256-CCM
- ECDHE-ECDSA-ARIA256-GCM-SHA384

- ECDHE-ARIA256-GCM-SHA384
- DHE-RSA-ARIA256-GCM-SHA384
- DHE-DSS-ARIA256-GCM-SHA384
- ARIA256-GCM-SHA384
- ECDHE-ECDSA-AES128-CCM8
- DHE-RSA-AES128-CCM8
- AES128-CCM8
- ECDHE-ECDSA-AES128-CCM
- DHE-RSA-AES128-CCM
- AES128-CCM
- ECDHE-ECDSA-ARIA128-GCM-SHA256
- ECDHE-ARIA128-GCM-SHA256
- DHE-RSA-ARIA128-GCM-SHA256
- DHE-DSS-ARIA128-GCM-SHA256
- ARIA128-GCM-SHA256
- ECDHE-ECDSA-CAMELLIA256-SHA384
- ECDHE-RSA-CAMELLIA256-SHA384
- DHE-RSA-CAMELLIA256-SHA256
- DHE-DSS-CAMELLIA256-SHA256
- ADH-CAMELLIA256-SHA256
- CAMELLIA256-SHA256
- ECDHE-RSA-CAMELLIA128-SHA256
- DHE-RSA-CAMELLIA128-SHA256
- DHE-DSS-CAMELLIA128-SHA256
- ADH-CAMELLIA128-SHA256
- CAMELLIA128-SHA256
- DHE-RSA-DES-CBC3-SHA
- DHE-DSS-DES-CBC3-SHA
- DHE-RSA-AES256-CCM8
- ECDHE-ECDSA-CAMELLIA128-SHA256

The following old and vulnerable algorithms were removed. (All that use DH and ECDH.) You cannot turn them on in non-FIPS mode. Here is the full list:

- DH-DSS-AES256-GCM-SHA384
- DH-RSA-AES256-GCM-SHA384

- ECDH-RSA-AES256-GCM-SHA384
- ECDH-ECDSA-AES256-GCM-SHA384
- ECDH-RSA-AES256-SHA384
- ECDH-ECDSA-AES256-SHA384
- DH-DSS-AES256-SHA
- DH-RSA-AES256-SHA
- ECDH-RSA-AES256-SHA
- ECDH-ECDSA-AES256-SHA
- DH-DSS-AES256-SHA256
- DH-RSA-AES256-SHA256
- DH-DSS-CAMELLIA256-SHA
- DH-RSA-CAMELLIA256-SHA
- DH-DSS-AES128-GCM-SHA256
- DH-RSA-AES128-GCM-SHA256
- ECDH-RSA-AES128-GCM-SHA256
- ECDH-ECDSA-AES128-GCM-SHA256
- DH-DSS-AES128-SHA
- DH-RSA-AES128-SHA
- ECDH-RSA-AES128-SHA
- ECDH-ECDSA-AES128-SHA
- DH-DSS-AES128-SHA256
- DH-RSA-AES128-SHA256
- ECDH-RSA-AES128-SHA256
- ECDH-ECDSA-AES128-SHA256
- DH-DSS-SEED-SHA
- DH-RSA-SEED-SHA
- DH-DSS-CAMELLIA128-SHA
- DH-RSA-CAMELLIA128-SHA
- DHE-DSS-RC4-SHA
- ECDH-RSA-RC4-SHA
- ECDH-ECDSA-RC4-SHA
- DH-DSS-DES-CBC3-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DH-RSA-DES-CBC3-SHA

- ECDH-RSA-DES-CBC3-SHA
- ECDH-ECDSA-DES-CBC3-SHA

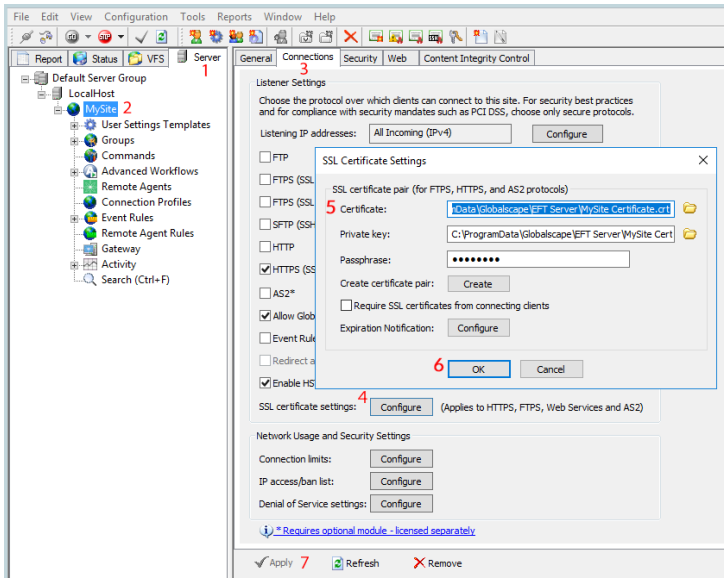
Also note, that "Export" status is a very outdated concept and is no longer supported by OpenSSL. This option is removed.

Assigning a Certificate to an EFT Site

An SSL Certificate is necessary for FTPS, HTTPS, and AS2 connections. After you create or obtain an SSL certificate, you can assign the certificate to one or more Sites.

To assign a certificate you have created or obtained to a Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. Click the Site you want to configure.
3. In the right pane, click the **Connections** tab.
4. In the **SSL certificate settings**area, click **Configure**. The **SSL Certificate Settings** dialog box appears.



   - To create a certificate, click **Create**and follow the prompts in the wizard. (Refer to Creating Certificates for details, if necessary.)
   - To use an existing certificate:
     a. In the **Certificate**box, type the path to the **.crt**file or click the folder icon to find and select it.
     b. In the **Private key** box, type the path to the **.key**file or click the folder icon to find and select it.
     c. In the **Certificate passphrase** and **Confirm passphrase** boxes, type and confirm the passphrase for the certificate pair.
5. Select the **Require SSL certificates from connected clients** check box, if you want connecting clients to use an SSL certificate.

6. To configure certification expiration notifications, refer to SSL Certificate Expiration Notification.
7. Click **OK** to close the dialog box.
8. Click **Apply**to save the changes on EFT.

Certificate Chaining

A *certificate chain* is used to establish a chain of trust from a peer certificate to a trusted CA certificate. Each certificate is verified using another certificate, creating a chain of certificates that ends with the root certificate. The issuer of a certificate is called a *certification authority* (CA). The owner of the root certificate is the *root certification authority*. The last certificate in the chain is usually a self-signed certificate.

EFT supports full certificate chains, which is a single file with a combination of all certificates in the chain. Usually, you will receive this file from a signing authority. Otherwise, you can create the chain manually, as described below, or ask the Globalscape Technical Support team to create one for you.

To create the chain, the general steps include:

1. You must have the following certificates:
    - Client/server certificate signed with the intermediate CA certificate
    - One (or more) intermediate CA certificates
    - A root CA certificate
2. Download the OpenSSL command line utility, available free from http://www.openssl.org/related/binaries.html.
3. Run the **x509** command on a certificate file, outputting the text version of that file. (Refer to the example below.)
4. Redirect the output into a *combined* file as a concatenated block of text.

For example, suppose you created a certificate in EFT called "mycert.crt" (and it has the associated private key "mycert.key"), then sent the CSR file ("mycert.csr") to Verisign, who sent you the following:

- Signed certificate ("mycert_Signed.crt")
- Intermediate certificate ("Verisign_Intermediate.crt")
- Root certificate ("Verisign_Root.crt").

To combine these into a single file that EFT supports, use the following commands in OpenSSL:

```
c:\> openssl x509 -inform PEM -in "mycert_Signed.crt" -text >
mycert_combined.crt
        c:\> openssl x509 -inform PEM -in "Verisign_
Intermediate.crt" -text >> mycert_combined.crt
        c:\> openssl x509 -inform PEM -in "Verisign_Root.crt" -
text >> mycert_combined.crt
```

You now have a certificate file that EFT can use to deploy the entire chain.

The way you access the intermediate and root certificates, as well as the format of those certificates, might differ between signing authorities.

Related Topics

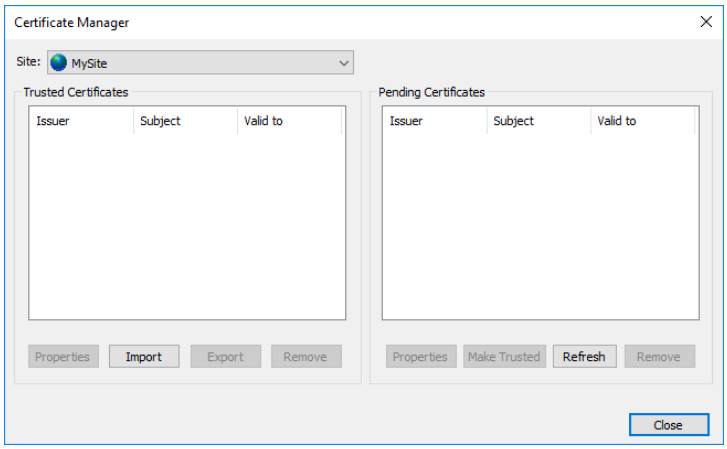
- Creating Certificates
- Assigning a Certificate
- Signing a Certificate
- Importing a Certificate

Certificate Manager

The **Certificate Manager** is used to manage the SSL certificates for a Site. The **Certificate Manager** browses your **My Documents**folder by default when you click **Import**or **Export**. For a client to connect to the server, their certificate must appear in the **Trusted Certificates** list.

To open the Certificate Manager

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the main menu, click **Tools > Manage SSL Certificates**. The **Certificate Manager** appears.



   - To view all of the certificates for a Site, click the **Site** drop-down list to select the Site. The certificates for the selected Site appear.
   - To view the properties of a certificate, click the certificate in the list, and then click **Properties**. The **Certificate Contents**dialog box appears, showing the **Issuer**and **Subject** information and the dates the certificate is valid.
   - To import certificates for a Site, refer to Importing a Certificate.
   - To export certificates from a Site, refer to Exporting a Certificate.
   - To remove a certificate, click the certificate in the list, and then click **Remove**.
   - To create a new certificate, refer to Creating Certificates.
   - To move a certificate from the **Pending**to the **Trusted** list, click the certificate and then click **Make Trusted**.
3. Click **Close**to close the Certificate Manager.

Related Topics

- Importing a Certificate
- Exporting a Certificate
- Creating Certificates
- Assigning a Certificate

Creating SSL Certificates

A *self-signed certificate* contains a public key, information about the owner of the certificate, and the owner's signature. It has an associated private key, but it does not verify the origin of the certificate through a third-party certificate authority.

To achieve the highest level of authentication between critical software components, do not use self-signed certificates, or use them selectively.

A certificate on the client must be associated with EFT to initiate an SSL connection. When you are administering EFT on the local computer, you can import your own certificates or create new ones using the **Certificate Creation Wizard** (described below).

EFT does not support SSL Certificate Private Keys without passphrases.

Three types of files are associated with an SSL certificate key pair:

- **Private key file**- The private key should never be distributed to anyone. It is used to decrypt the session, which is encrypted by the public key. Available formats include:
  - PEM (ASCII) encoded - *.key
  - PKCS#12 (PFX combined) - *.pfx (not available when in FIPS mode)
  - DER (binary private key) - *.der
- **Certificate file** - This is a signed certificate, whether self-signed or signed by an intermediate certificate authority. Available formats include:
  - PEM (ASCII) encoded - *.crt
  - PKCS#7 (P7B public key) - *.p7b
  - DER (binary public key) - *.cer
- **Certificate signing request file (.csr)** - Each time you create a certificate using EFT, a Certificate Signing Request file is also created. A Certificate Signing Request (CSR) is an unsigned copy of your certificate. This file can be signed by EFT's **Certificate Signing Utility** or sent to an intermediate certificate authority, such as GeoTrust, for signing.

For maximum compliance with security standards, you should use a trusted authority signed SSL certificate. You can import certificates or use this wizard to create your own. The private key (.key) and certificate request (.csr) files are created at the same time. You are prohibited from creating certificates for EFT while remotely administering EFT because this Action can create a security breach. Any certificates

you create remain on the computer on which you create them, unless you take special steps to deliver and associate these files with another computer.

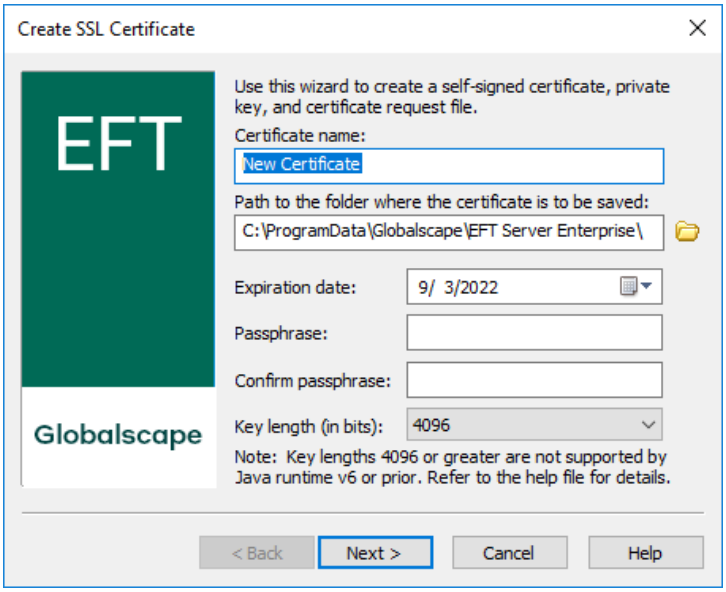
The Certificate Creation Wizard does not create SHA-2 certificates; however, EFT can apply a SHA-2 certificate generated through other means, like certificate authorities and third party applications.

> **NOTE:** EFT can only create detached signature files; however, it can verify signatures for non-detached, detached, and XML-Enveloped signature files.
> The current build of EFT does not provide a mechanism to "decrypt" the file created with the signing process.
> The current build of EFT does not provide "Browse" objects for the TEXT boxes. (This is a limitation in the EFT Arcus environment.)

To create an SSL certificate

1. In the administration interface, connect to EFT, click the **Server**tab, then do one of the following:
   - On the main menu, click **Tools > Create SSL Certificate**.
   - On the toolbar, click the **New SSL Certificate**icon .
   - On the keyboard, press ALT+T+C.

   The **Create SSL Certificate**wizard appears.

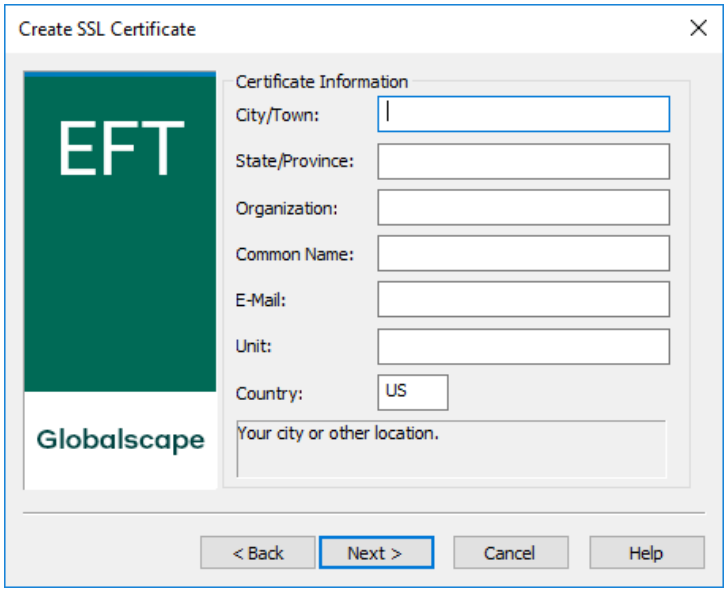


2. In the **Certificate name** box, specify the name (up to 256 characters) of the certificate that will be generated.

3. In the **Path**box, specify the path to the folder in which the certificate is to be saved. The wizard saves each of the files in this folder.

   If you are purchasing a signed certificate from a certificate authority (CA), you usually need to forward the contents to the CA. To do this, locate the .csr and open it in a text editor. Then you can copy and paste the contents.

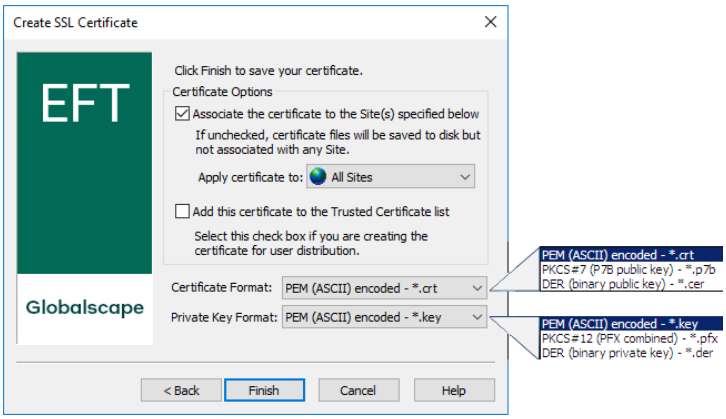
4. In the **Expiration Date** box, specify the date on which the certificate will expire.
5. In the **Passphrase**and **Confirm passphrase** boxes, type the passphrase used to encrypt the private key. The passphrase can be any combination of characters or spaces. Do not lose the passphrase; the certificate is useless without it.
6. In the **Key Length**(in bits) box, specify the key length: 512, 1024, 2048, and 4096 bits. Smaller keys are faster, larger keys are more secure.
7. Click **Next**. The **Certificate Information**page appears.



   Each of the boxes must be completed before continuing. The information you provide is stored in the certificate.

8. In the **City/Town**box, provide the name of your city, town, or other locality.
9. In the **State/Province**box, provide the name of the state or province.
10. In **Organization**box, provide the name of your organization, or any other designator.
11. In the **Common Name**box, provide the common name or fully qualified domain name, such as www.globalscape.com. (Typically, the name or domain name associated with the Site.)

12. In the **email**box, provide your email address in the format *username@domain.com*.
13. In the **Unit**box, type any other information about your organization, such as department name.
14. In the **Country**box, provide the 2-letter ISO country code using uppercase letters.
15. Click **Next**. The **Certificate Options** page appears.



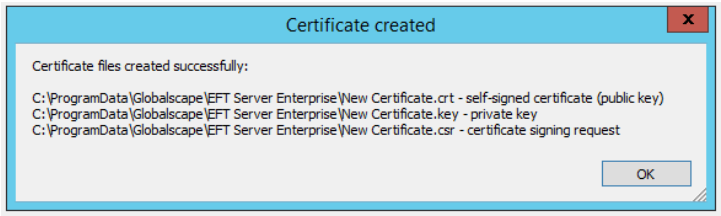
16. If the **Associate the certificate to the Site(s) specified below** check box is cleared, the wizard saves only the certificate files in the folder you previously specified, but does not associate it with any Site. If the check box is selected, the wizard associates the certificate to the administration service or Site(s) you specify in the **Apply certificate to** box.
17. In the **Apply certificate to** box, specify which components of EFT are affected (**administration Service**, **All Sites**, or a specific Site).

    Associating a new certificate with a Site requires a restart of the Site, and any active users will be disconnected, so it is recommended that you associate certificates when Sites are inactive or stopped.

18. If the **Add this certificate to the Trusted Certificate list** check box is selected, the wizard adds the certificate to the Trusted Certificates database. Use this feature if you are creating certificates for user distribution. You can limit EFT access to just the users that have the certificate. You can verify the addition to the Trusted Certificate database by clicking **Tools >Certificate Manager** or, on the toolbar, click the **Certificate Manager**icon . (Refer to The Certificate Manager for more information.)
19. In the **Certificate Format** box, specify the format of the certificate file.
20. In the **Private Key Format** box, specify the format of the key file.

> **NOTE:** PKCS12 (pfx) format is not available when in FIPS mode.

21. Click **Finish**. The certificate is created and a message box appears. You can select and copy the certificate information, if desired, and then click **OK** to dismiss the message.



22. Refer to ***Enabling SSL on the Site* on page 424** and ***Enabling SSL on the Server* on page 422** for instructions for using the SSL certificate.

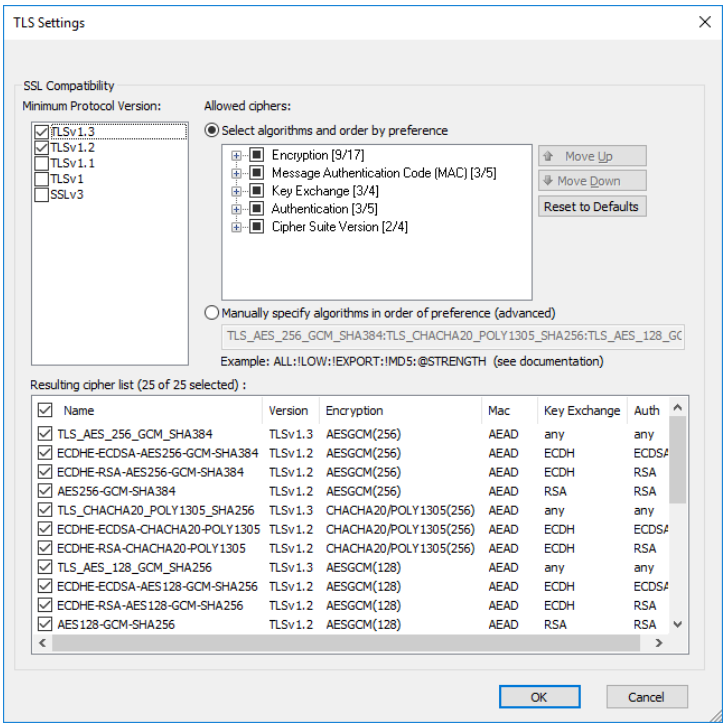
Enabling SSL on the Server

Before configuring SSL on the Site, you must configure SSL on the server. Specify SSL versions and ciphers before enabling SSL connections. After you have enabled SSL for the server, SSL connections can be enabled on the Site, Settings Template, and/or for each user. Each level can inherit the settings from the parent.

> **NOTE:** To disable TLS 1.3 or any other TLS version, you must clear the check box for the protocol version from the **Minimum Protocol Version** box and not just clear all the cipher versions from the **Resulting cipher list** box. EFT must have at least one cipher suite enabled (under the **Resulting cipher list** window) that is compatible with the highest enabled TLS version (under the **Minimum Protocol Version**), else TLS/SSL connections will fail. See also TLS 1.3 Support.

To configure SSL

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the server node that you want to configure.
3. In the right pane, click the **Security**tab.
4. Next to **SSL security settings**, click **Configure**. The **TLS Settings** dialog box appears.



5. Select the check box of one or more ciphers/algorithms to use, or manually specify the ciphers. At least one cipher must be specified.
    - Only advanced users should manually specify ciphers.
    - SSL Cipher and Version-allowed settings affect ALL Sites on EFT.
    - For PCI DSS compliance, EFT checks for 128-bit or higher ciphers, and SSLv3 or greater, and no use of CCC or PROT-C.
    - A Certificate Authority (CA)-signed certificate establishes your validity better than a self-signed certificate.
    - For details of SSL when using FIPS mode, refer to FIPS-Certified Library.
6. Click the arrows to arrange the ciphers in top-down priority. If more than one approved cipher is specified, and the connecting client has in its list one or more ciphers that are also on EFT's approved list, EFT will select and use the cipher based on ordering (priority) shown in the list box.
7. Click **Apply**to save the changes to EFT.

Enabling SSL on the Site

Specify SSL versions and ciphers before enabling SSL connections. SSL must first be enabled on EFT and Site, then can be enabled in the Settings Template and user.

You can inherit the TLS settings from the server, or specify different settings on the site.

See also Enabling SSL on the Server and TLS 1.3 Support.

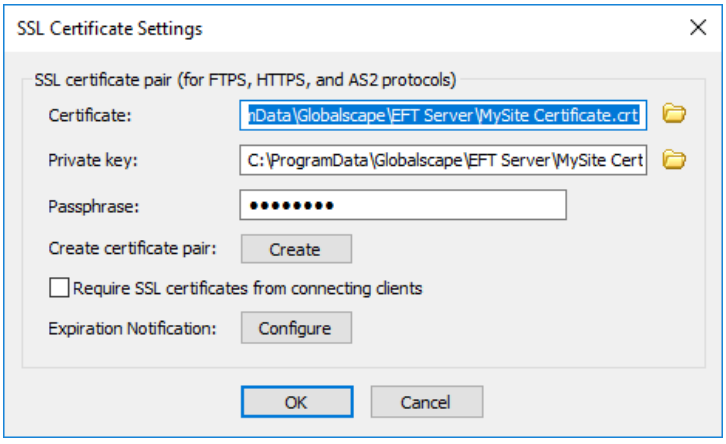
If you require certificates from connecting clients before they can connect, then their certificate must be in the Trusted Certificates Database or signed by a certificate in the Trusted Certificate Database.

If you are using SSL authentication for accounts that need to send AS2 transfers, leave it at the default password authentication, not certificate authentication.

EFT does not support SSL Certificate Private Keys without passphrases.

To enable SSL and assign the certificate

1. In the administration interface, connect to EFT and click the **Server**tab.
2. Click the Site you want to configure.
3. In the right pane, select the **Connections** tab, then select the applicable protocol check boxes (FTPS, HTTPS, and/or AS2).
4. In the **SSL certificate settings** area, click **Configure**. The SSL Certificate Settings dialog box appears.



Refer to Assigning a Certificate for details of configuring SSL.

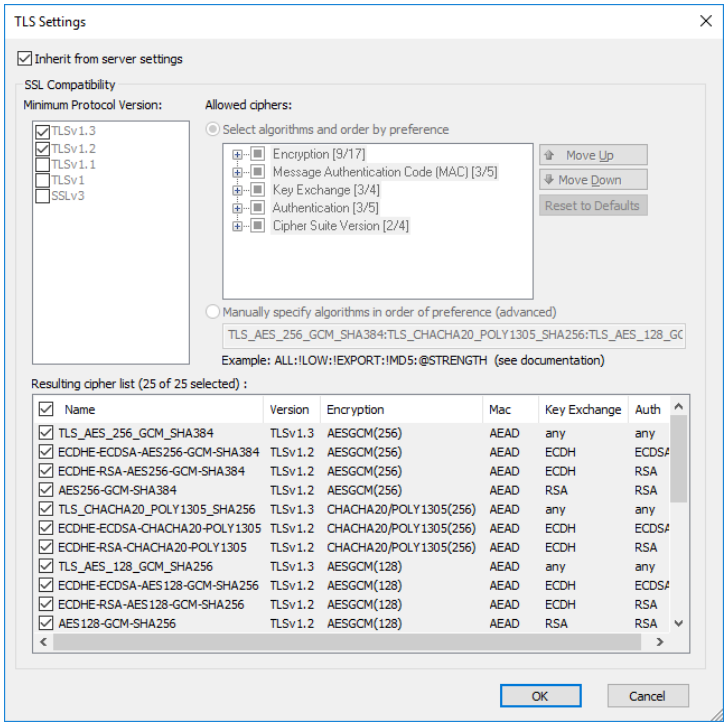
5. Click **OK** to close the dialog box.
6. Click **Apply**to save the changes to EFT.

TLS Settings on the Site

On a Site's **Connections** tab, you can configure TLS settings specifically for that Site, or choose to inherit the settings from the server, which is the default.

To specify TLS settings on the Site

1. In the administration interface, connect to EFT and click the **Server**tab.
2. Click the Site you want to configure.
3. In the right pane, select the **Connections** tab, then select the applicable protocol check boxes (FTPS, HTTPS, and/or AS2).
4. Next to **SSL security settings**, click **Configure**. The **TLS Certificate Settings** dialog box appears.



5. The **Inherit from server settings** check box is selected by default. If you need to specify different settings for this Site, clear the check box, then select or clear the **Minimum Protocol Version** to use, the **Allowed ciphers**, and the **Resulting ciphers**.

Refer to ***TLS 1.3 Support* on page 405**and ***Enabling SSL on the Server* on page 422** for more information on specifying these settings.

Configuring SSL Authentication for a Settings Template or User Account

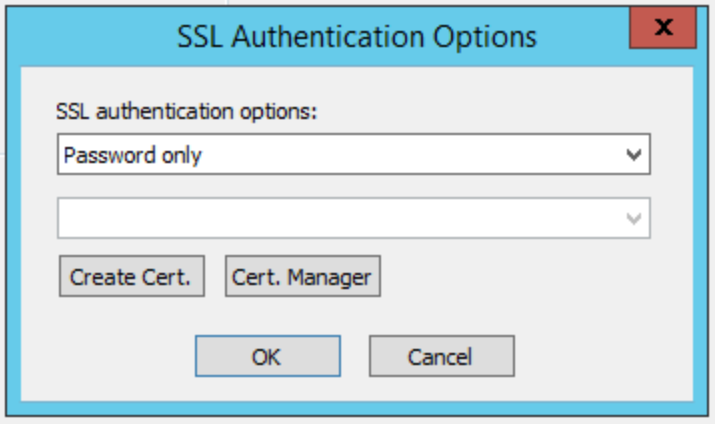
SSL must first be enabled on the Siteand Server. SSL authentication can then be enabled for a Settings Template and/or for each user.

If you require certificates from connecting clients before they can connect, then their certificate must be in the Trusted Certificates Database or signed by a certificate in the Trusted Certificate Database.

If you are using SSL authentication for accounts that need to send AS2 transfers (requires optional module), leave it at the default password authentication, not certificate authentication.

To enable SSL

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, select the Settings Template or user account that you want to configure.
3. In the right pane, select the **Connections**tab.
4. In the **Protocols**area, select the applicable check boxes (FTPS, HTTPS, and/or AS2).
5. Click **SSL Auth**. The **SSL Authentication Options** dialog box appears.



6. In the **SSL authentication options** list, specify the authentication method:
   - **Specified in Settings Template** (available for user accounts)
   - **Password only**

- **SSL Certificate**- If SSL Certificate is specified, specify the user certificate in the second list that appears.

  Compliance with PCI DSS requires that users change their password upon initial login. Because the "SSL Certificate" login method does not use a password, it potentially violates the PCI DSS and is, therefore, not available on Sites defined using the "strict security settings" option.

7. Click **OK** to close the dialog box.
8. Click **Apply**to save the changes to EFT.

Exporting a Certificate

For expediency, you should save the certificates that you want to export into EFT in your **Documents** folder. The **Certificate Manager** browses the **Documents** folder by default when you click **Export**.

To export a certificate from the database

1. On the main menu, click **Tools > Manage SSL Certificate**. The **Certificate Manager** dialog box appears.
2. In the **Trusted Certificates**list, click **Export**, and browse to the folder where you want to save the certificate file.
3. Type a name for the certificate file, and then click **Save**.

Exporting a Certificate from PFX to PEM

For security, EFT does not allow you to use a certificate file with a **.p*** (for example, **pfx**, **p12**) extension. The **.p*** extension indicates that it is a combined certificate that includes both the public and private keys, giving clients access to the private key. You can create certificate files using EFT's Certificate wizard. If you have a combined certificate from a third-party, use the procedure below to extract the public key.

To export the certificates from PFX to PEM

1. Download the precompiled Windows binary and Windows Installer for OpenSSL from http://www.slproweb.com/products/Win32OpenSSL.html. The OpenSSL distribution contains a number of utilities, including the main utility **openssl.exe**. By default, the utilities are installed in **C:\Openssl\bin**.
2. Open a Windows command prompt and navigate to **\Openssl\bin**.
3. Type `openssl.exe` and press ENTER. The OpenSSL prompt appears.
4. Execute the following command:

   ```
   pkcs12 -in <cert.pfx> -out <cert.pem> -nodes
   ```

   where <cert.pfx> is the name of the PFX file (you might need to include the path and quotes), and <cert.pem> is the name of the file that OpenSSL is to generate (include the path if you want to save it in a location other than **\Openssl\bin**.)

   For example, type:

   ```
   pkcs12 -in "C:\Program Files\nsoftware\IPWorks EDI V7 AS2 Connector\as2datacert.pfx" -out cert.pem -nodes
   ```
5. The command converts the data in the <cert.pfx> file to PEM format in the <cert.pem> file. The PEM file contains all of the certificates that were in the PFX file:
   - Private key
   - Identity certificate
   - Root certificate
   - Intermediate certificate

   Each of the certificates (Private Key, Identity certificate, Root certificate, Intermediate certificate) is wrapped within headers, and these headers are part of the certificates. The PEM file looks similar to the following:

```
Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: 6334386951390085 99
    Microsoft CSP Name: Microsoft Base Cryptographic Provider v1.0
Key Attributes
    X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC2izwuMKflSVlks3KNcEN5oagzvGnwjLL9HOpBaqd9gkcHzZmc
TlGiLreKWaOxbR2BMIEHkYC2GzVjBcQUSz/QOYYOBrbg+hoBvrCt547cPSqSBQdL
BLebYWEqua7R25R80yiMfTwZwQB0+DHD+pDlXAB9AN/ENjGyc4VPU+A6/QIDAQAB
AoGBAKGJZzEM16TlStklP2rQfLWHC7z0r98x8zax2Nk404zqm4bZN2Uuf/QAWWVx
27yn7aMkVBppdTgxrbW6JYE78fQH2kx5D3RtJYpgULmYkp2MHGlgfuPVtMVReS+R
JuXP47ysQVROGMwUftgANpov9Mx/lGU36CF/oiG7cjIyMpElAkEA4sDJqFvKOfGF
MOsUCUOL2A+RRjKNQ3bTgt5o8LNu6uRh3ztbsKB+J+FvNArRWU4Ftgn3U7q7BwT9
Aabte2pnRwJBAM4WsaKsnvTEM/oByMbFJO360AbLSx7e3q44zl9xAtlWwxPh/mn7
RD6oKDhf61ML+kfGGFzHV99UCrca9aFeNZsCQQDg8m5bhcvllbMTJ3J2CjtWOYNe
BlJapiwIPQoQF4GmprBtW56HZ4AfoiXGlCDBHoTN5a8lsi50NWWlWOtpLtKLAkBq
jVkyXkWhD4BAFoQUIQL9UlwT5y/juh8vvLcWqXtrm2wo74N2kC7spkyFOTIRlfOF
AGrALWDFWtJfcVTmJatZAkBGg3Uk6sTOjdw0NbkG57DRITMNrrHjJ2xuLO0dEfjS
e3EUmPOiaY7m6c/2EqvB+wRDl/2HUaBId0u2woDis30T
-----END RSA PRIVATE KEY-----
Bag Attributes
    localKeyID: 01 00 00 00
subject=/CN=EDI Connector Cert
issuer=/CN=EDI Connector Cert
-----BEGIN CERTIFICATE-----
MIIBrjCCARegAwIBAgIBATANBgkqhkiG9w0BAQUFADAdMRswGQYDVQQDExJFREkg
Q29ubmVjdG9yIENlcnQwHhcNMDgwNDE1MjAxODM0WhcNMDkwNDE0MjAxODM0WjAd
MRswGQYDVQQDExJFREkgQ29ubmVjdG9yIENlcnQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALaLPC4wp/VJWWSzcolwQ3mhqDO8afCMsv0fSkFqp32CRwfNmZxP
UaIut4pZo7FtHYEwgQeRgLYbNWMFxBRLP9A5hg4GtuD6GgG+sK3njtw9KpIFB0sE
t5thYSq5rtHblHw7KIx9PBnBAE74McP6kPVcAHOA38Q2MbJzhU9T4Dr9AgMBAAEw
DQYJKoZIhvcNAQEFBQADgYEALdwDjY/epA6t63cAcLfdVhv+hRSh+wqkkX6x4IPA
jL0Jyx0rTPKEcqlMd8NMXiOhGNUhR5hl4IpSvQlW92Xeq5WMmfiklfDhOBczgBjX
KplhndxyWFeJ6o/9xmSKr0ctNPi+//n/Y9ADNaP2iz+sgD0gicLaPaljGMDgxEUN
MlY=
-----END CERTIFICATE-----
```

6. Open the PEM file in a text editor (NotePad, EditPlus) and delete all but the last certificate section so that the file only contains the section that starts

   `-----BEGIN CERTIFICATE-----`

   and ends

   `-----END CERTIFICATE-----`

7. Save the file with a **.crt** extension. The file is now ready to be used in EFT for the partner certificate.

Refer to Knowledgebase article Using OpenSSL to Generate/Convert Keys and Certificates for more information regarding using the OpenSSL command-line tool to generate and convert private keys and public certificates.

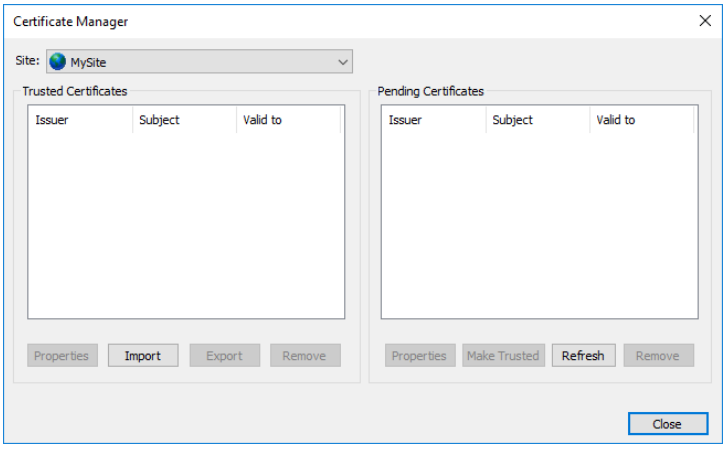
Importing a Certificate

For expediency, you should save the certificates that you want to import into EFT in your **My Documents**folder. The **Certificate Manager**browses your **My Documents** folder by default when you click **Import**.

If you attempt to import a certificate that has a key length of 512 bits or less on a Site created using the "strict security settings" option, EFT prompts you that only strong keys should be used. You are offered the option of importing a key that has at least 1024 bits or continuing with reason.

To import a certificate to a Site

1. On the main menu, click **Tools >Manage SSL Certificat**e. The **Certificate Manager** appears.



2. In the **Trusted Certificates**list, click **Import**.
3. Browse to the folder that contains the client's certificate file and click the file.

   EFT can import a digital certificate from the following formats: PEM, Base64 Encoded X509, DER Encoded X509, PKCS#7, PKCS#12.

   The private key associated with the digital certificate must be in one of the following formats: PEM, DER, PKCS#8, PKCS#12.

   A Certificate Signing Request (.csr) is a PKCS10 request, which is an unsigned copy of your certificate.

4. Click **Open**. EFT automatically determines the certificate format. If EFT is unable to determine the format, or if the import fails, you can manually convert a digital certificate to one of the above formats and import it. Consult the distributor/vendor of your certificate for details on this process.

The certificate is added to the Trusted Certificates database. Clients submitting that certificate are now able to connect to EFT.

Related Topics

- Exporting a Certificate from the Trusted Certificate Database
- SSL

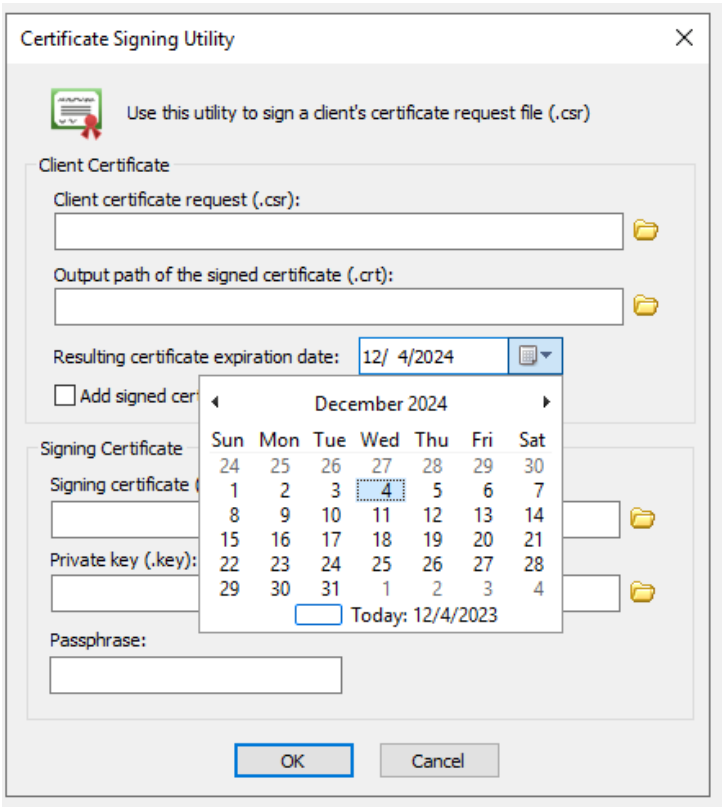
Signing a Certificate

EFT can sign certificate requests created by other clients. Typically, the client certificate request is signed with the certificate created for EFT. If a certificate from the FTP server's Trusted Certificates database is used to sign client certificates, then all certificates you sign are automatically trusted.

EFT checks the key length and expiration date only for EFT's SSL certificates (that is, administration certificate and Site certificates); client certificates (that is, trusted certificates) are not checked.

To sign a certificate request

1. Obtain the Certificate Signing Request file. This can be done through email or any other file delivery method.
2. In the administration interface, connect to EFT and click the **Server**tab.
3. On the **Server**tab, click the Server or a Site node.
4. On the main menu, click **Tools > Sign SSL Certificate**, or click the **Certificate Signing Utility** icon . The **Certificate Signing Utility** dialog box appears.



5. In the **Client certificate request** box, click the folder icon to browse for and specify the Certificate Signing Request file that you want to sign.

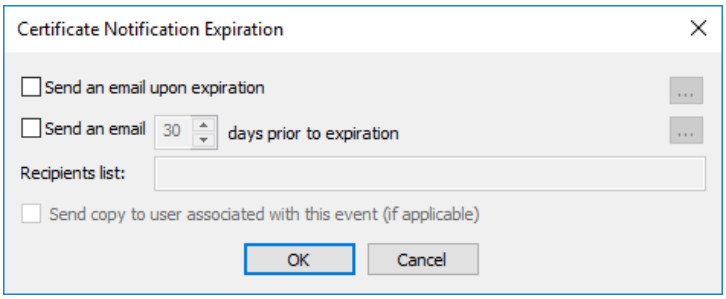
6. In the **Output path** box, click the folder icon to browse for and specify the folder in which to save the signed certificate file.
7. In the **Resulting certificate expiration date** box, click the list to open a calendar in which to specify an expiration date.
    - Click the left- and right-facing arrows to scroll through the months.
8. In the **Signing certificate** box**,** specify the certificate that you want to use to sign the certificate request file. The signing certificate must be in your trusted certificate database in order for clients submitting the signed certificate to connect to the Site.
9. In the **Private key** box, specify the private key file associated with the signing certificate.
10. In the **Passphrase** box, provide the passphrase associated with the signing certificate.
11. Click **OK**. The new certificate is saved in the folder you specified.
12. Return the certificate file to the user.

SSL Certificate Expiration Notification

An SSL Certificate is necessary for FTPS, HTTPS, and AS2 connections. After you create or obtain an SSL certificate, you can assign the certificate to one or more Sites.

To assign a certificate you have created or obtained to a Site

1. In the administration interface, log in to EFT and click the **Server** tab.
2. Click the Site you want to configure.
3. In the right pane, click the **Connections** tab.
4. In the **SSL certificate settings**area, click **Configure**. The **SSL Certificate Settings** dialog box appears.
5. Next to **Expiration Notification**, click **Configure**. The **Certification Notification Expiration** dialog box appears.



   a. Select a check box to **Send an email upon expiration** and/or **Send an email N days prior to expiration**.
   b. Specify one or recipients to receive the notifications, separate email addresses by commas.
   c. Select the check box if you want to **Send copy to user associated with the event, if applicable**.
   d. Click **OK**.

> **NOTE:** For email notifications to work for SSL Certificate Rotation Period Notification the SMTP tab of the serverneeds to be configured properly.

6. Click **OK** to close the dialog box.
7. Click **Apply**to save the changes on EFT.

SSL Certificate-Based Login

EFT supports authentication using SSL certificates for FTPS, and HTTPS, and AS2 connections, rather than password-based login. This is similar to SFTP authentication in which a particular SFTP key is associated with a user account; when the user logs in and provides the key, as long as the keys match, they are allowed to proceed. Unlike SFTP, SSL offers the option to authenticate using both password and certificate rather one or the other.

Normally, when a client supplies an SSL certificate for the SSL handshake (if requested by EFT), EFT determines whether that certificate is in the global trusted list. If the certificate is trusted, EFT completes the process of negotiating a shared secret and then moves on to the authentication stage, requesting a username followed by a password. If the user enters the wrong password (or no password at all), the authentication attempt fails, even though a certificate was found in the trusted store that matched the client's certificate.

EFT determines whether certificate keys used on EFT are current and reports the status in the PCI DSS Compliance Report. Refer to Possible Compliance Report Outcomes for more information.

With certificate-based authentication, the sequence of steps would be virtually the same. If certificate-based authentication is enabled, and after the client's username has been provided, but prior to EFT requesting the user's password, EFT verifies that the public key of the provided certificate matches the certificate in the trusted store that is associated with (mapped to) this particular user's account. If a match is made, that user is automatically authenticated for that session. If the protocol expects a username/password sequence, EFT always returns TRUE, regardless of the password supplied by the client (whether null or invalid pass).

Compliance with PCI DSS requires that users change their password upon initial login. Because this login method does not use a password, it potentially violates the PCI DSS and is, therefore, not available on Sites defined using the "strict security settings" option.

The procedures below describe how to specify SSL-based logins for Site, Settings Template, and user accounts.

To specify SSL certificate-based logins for the Site

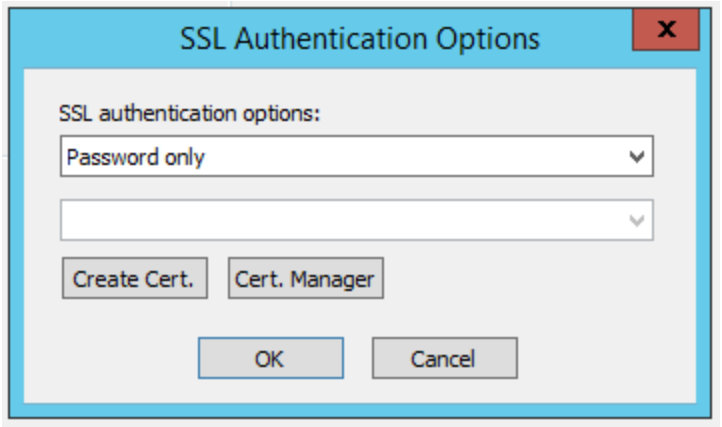
1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site that you want to configure.
3. In the right pane, click the **Connections**tab.

4. Next to **SSL certificate settings**, click **Configure**. Refer to Assigning a Certificate for details of configuring SSL.
5. Click **OK** to save the changes.
6. Click **Apply**to save the changes on EFT.

To specify SSL certificate-based logins for the Settings Template or a User

Do not specify SSL authentication options for accounts that need to send AS2 transfers. EFT's HTTP/S protocol handler requires a username and password at the outset of HTTP/S-based AS2 transactions.

1. In the administration interface, connect to EFT and click the **Server**tab.
2. Click the **Settings Template** or **user** that you want to configure.
3. In the right pane, click the **Connections**tab.
4. Select the **FTPS (SSL/TLS)**check box, if not inherited from the Site, and then click **SSL Auth**. The **SSL Authentication Options** dialog box appears.



5. In the **SSL authentication options** list, specify the authentication method:
   - **Specified in Settings Template** (if the user account is selected)
   - **Password only**(the default for the Settings Template)
   - **SSL Certificate**- If **SSL Certificate** is specified, the bottom box becomes available. Certificates that are defined on the Site appear in the box. Click the user certificate in the box. If no certificate is available:
     a. If you need to define a certificate, click **Create Cert**. The Create SSL Certificate wizard appears.
     b. To view or import certificates, click **Cert. Manager**. The Certificate Manager appears.
6. Click **OK** to close the dialog box.
7. Click **Apply**to save the changes on EFT.

Related Topics

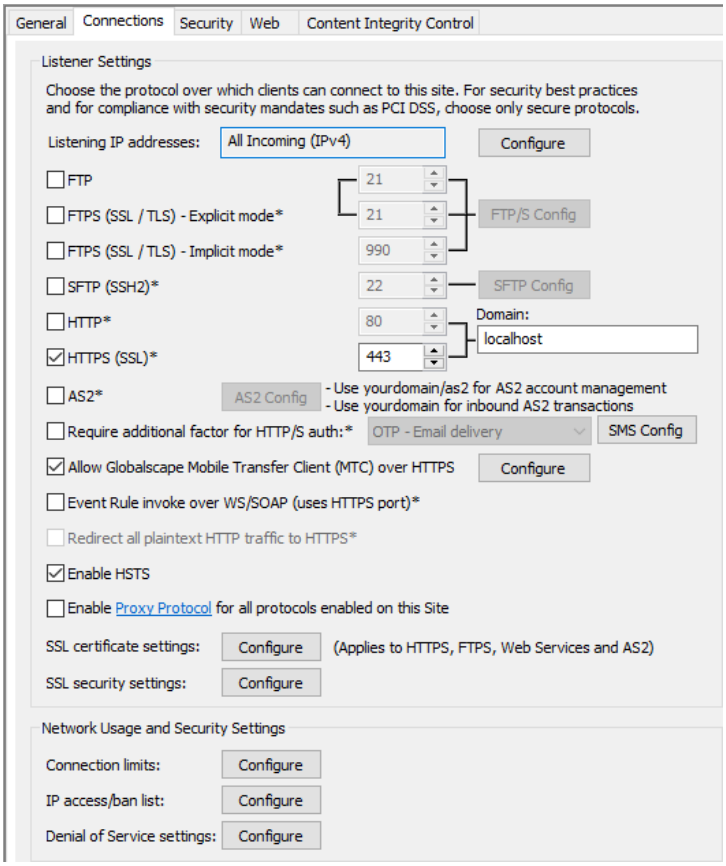
- Creating Certificates
- Assigning a Certificate
- The Certificate Manager
- Enabling FTPS, HTTPS (SSL) on the Site
- The AS2 Module

Disabling SSL Connections on the Site

You can disable SSL support for every user on EFT by disabling SSL support on the Site or you can disable SSL for a specific user or Settings Template. (See also Configuring SSL on the Server.)

To disable SSL connections

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site, Settings Template, or user for which you want to disable SSL.
3. In the right pane, click the **Connections**tab.



4. Clear the **FTPS (SSL/TLS) - Explicit mode**, **FTPS (SSL/TLS) - Implicit mode**, and **HTTPS**check boxes. At least one of the non-SSL protocol check boxes (FTP, SFTP, HTTP, AS2) must be selected or inheriting the parent settings.
5. Click **Apply**to save the changes on EFT.

   If SSL connections are disabled on the Site, they are also disabled for all Settings Templates and users on the Site.

Using OpenSSL to Generate/Convert Keys and Certificates

These online topics provide the procedures for using OpenSSL to generate and convert keys and certificates for use in EFT.

- Using OpenSSL
- KB11030: Converting an EFT Certificate to PFX Format
- KB11037: Generating an Unencrypted Private Key and Self-Signed Public Certificate
- KB11038: Generating an Encrypted Private Key and Self-Signed Public Certificate
- KB11039: Generating a PKCS#12 Private Key and Public Certificate
- KB11040: Converting an Incompatible PKCS#12 Format File to a Compatible PKCS#12
- KB11041: Converting a PEM-Encoded PKCS#8 Format Encrypted Private Key to PKCS#8 Format
- KB11042: Converting a Traditional PEM Encoded Encrypted Private Key to PKCS#8 Format

Federal Information Processing Standard (FIPS)

FIPS mode is included in EFT. (Requires SSL/TLS or SFTP modules)

- FIPS-Certified Library
- Enabling FIPS Mode for SSL Connections
- Enabling FIPS Mode for SSH (SFTP) Connections
- FIPS Mode Event Messages
- SFTP FIPS

FIPS-Certified Library

The Federal Information Processing Standard (FIPS) Publication 140-2 specifies the security requirements of cryptographic modules used to protect sensitive information. When the EFT service is started, if FIPS is enabled, a message displays which protocols are in use and which of the protocols in use are FIPS certified. When you enable FIPS, the ciphers, key lengths/types, and hash lengths/types that are not FIPS-approved are not available, and an initialization routine executes a series of startup tests that set the cryptographic module into a FIPS-approved operational state.

For more information about the cryptographic module used by EFT, refer to Knowledgebase article Do you have a link to the certificate for your FIPS ciphers?

After you enable or disable FIPS mode, you must restart the EFT server service.

If a FIPS-approved state cannot be achieved when FIPS is enabled, all Sites will stop, and an error message appears in the Windows Event Log and the EFT administration interface. After you dismiss the message, the EFT administration interface closes.

- You can enable FIPS mode for:
  - inbound SFTP (SSH2)
  - inbound HTTPs/FTPs (SSL)
  - outbound HTTPs/FTPs (SSL) through Event Rules (except when using Advanced Workflows)
  - outbound client SFTP (SSH2) through Event Rules
- FIPS mode does ***not***apply to:
  - EFT administration interface connections
  - SSL-based COM API connections
  - Advanced Workflows-based HTTPs/FTPs (SSL)
  - Advanced Workflows-based SFTP (SSH2)
  - AS2 inbound nor outbound transactions; SSL connections for AS2 are through HTTPS sockets, so the AS2 transaction is over a FIPS tunnel; however, the encryption within the AS2 MIME payload is not FIPS approved.

The following changes to the Server > Security tab were made in the latest version of EFT.

SSH changes in FIPS mode	
SSH keys	• generate rsa keys less than 2048 bit prohibited • prohibited using other than rsa/dsa keys >= 2048 bits or ecdsa keys >= 224 bits (for both client and server) • EFT will display the message: "The provided SFTP key has an improper key length or type. FIPS 140-2 mode requires keys at least 2048 bits length for RSA or DSA (DSS) keys and at least 224 bits for ECDSA keys. Please specify an alternate key, or generate a new one using EFT's SFTP key creation wizard."
KEXes	• "diffie-hellman-group1-sha1" prohibited (for both client and server)
MACs	• "hmac-sha1-96" prohibited (for both client and server) • "hmac-sha1" enabled by default (for client)
SSH changes in non-FIPS mode	
SSH keys	• prohibit generation of RSA keys less than 2048 bit (in GUI only)
MAC	• "hmac-sha1" enabled by default (for client)

The functional for legacy sftp.dll was kept unchanged. In legacy FIPS mode, allowed keys are, for example,

1024bits <= rsa <= 4096bits or dsa 1024bits

and if you set another key, then GUI will show message:

"The provided SFTP key has an improper key length. FIPS 140-2 mode requires keys between 1024 and 4096 bits (inclusive) for RSA keys, or 1024 bits (exactly) for DSA (DSS) keys. Please specify an alternate key, or generate a new one using EFT's SFTP key creation wizard."

SSL changes	
in FIPS mode	• Generating RSA keys less than 2048 bit is prohibited • Using other than RSA/DSA keys >= 2048 bits or ecdsa keys >= 224 bits (for both client and server) is prohibited • EFT will display the message: "The SSL certificate has an improper key length. FIPS 140-2 mode requires keys at least 2048 bits length for RSA or DSA (DSS) keys and at least 224 bits for ECDSA keys. Please specify an alternate certificate, or generate a new one using EFT's SSL certificate creation wizard."
in nonFIPS mode	• Generating rsa keys less than 2048 bit (in GUI only) is prohibited

Related Topics

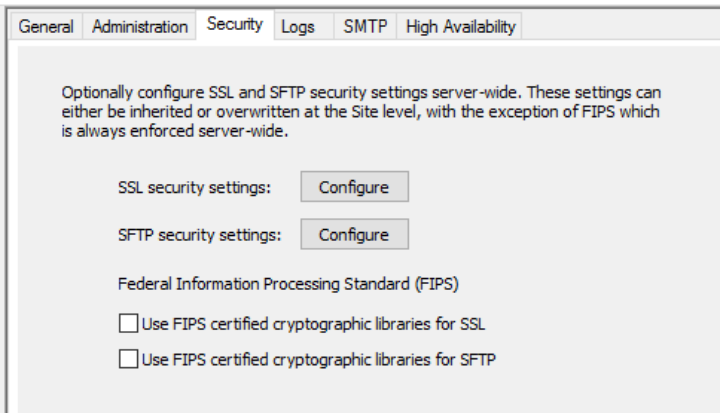
- Enabling FIPS Mode for SSL Connections
- Enabling FIPS Mode for SSH Connections
- FIPS Mode Event Messages

Enabling FIPS Mode for SSL (HTTPS and FTPS) Connections

After you enable or disable FIPS mode, you must restart the EFT server service. (You must have a Server administrator account in EFT to perform this procedure.)

To enable FIPS mode for SSL Connections

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node on which you want to enable FIPS mode.
3. In the right pane, click the **Security**tab.



4. In the **Federal Information Processing Standards (FIPS)** area, select the **Use FIPS certified cryptographic libraries for SSH connections**check box.
5. Click **Apply**to save the changes on EFT.

When the EFT Site is started, if FIPS is enabled, a message displays the protocols in use and which of the protocols in use are FIPS certified. When you enable FIPS, the ciphers, key, and hash lengths/types that are not FIPS-approved are not available. If a FIPS-approved state cannot be achieved when FIPS is enabled, all Sites will stop, and an error is written to the Windows Event Log.

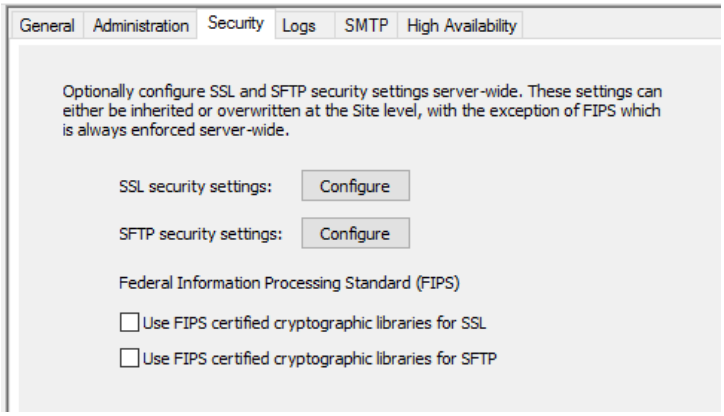
Imported certificates that were signed using non-FIPS-certified algorithms will not work in EFT when using FIPS mode. For details of converting certificates prior to importing them into EFT, refer to Using OpenSSL to Generate/Convert Keys and Certificates.

Enabling FIPS for SSH (SFTP) Connections

After you enable or disable FIPS mode, you must restart the EFT server service.

To enable FIPS for SSH connections

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node on which you want to enable FIPS mode.
3. In the right pane, click the **Security**tab.



4. In the **Federal Information Processing Standards (FIPS)** area, select the **Use FIPS certified cryptographic libraries for SSH connections**check box.
5. Click **Apply**to save the changes on EFT.
6. On EFT's **General**tab, review the **Statistics**area to verify that the service started.

When the EFT Site is started, if FIPS is enabled, a message displays the protocols in use and which of the protocols in use are FIPS certified. When you enable FIPS, the ciphers, key, and hash lengths/types that are not FIPS-approved are not available. If a FIPS-approved state cannot be achieved when FIPS is enabled, all Sites will stop, and an error is written to the Windows Event Log.

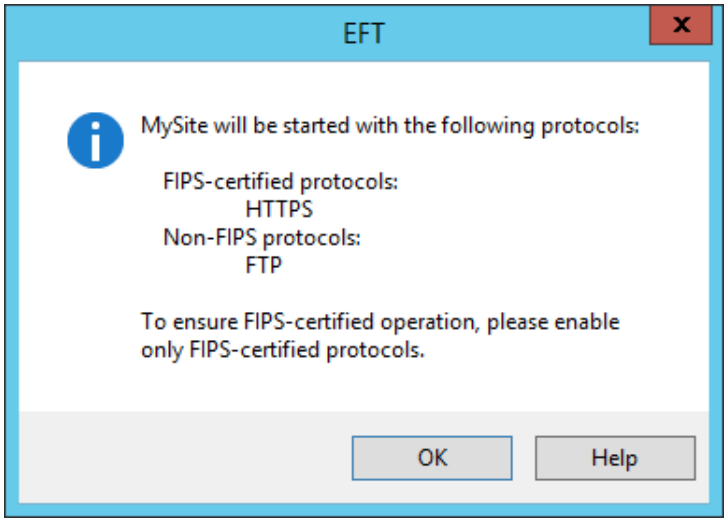
FIPS Mode Event Messages

EFT displays FIPS-related messages when switching to/from FIPS modes, starting/restarting EFT or Site, making administration interface connections, or managing certificates. EFT presents messages in the administration interface and in the Windows Event Log and allows you to correct the error. That is:

- A FIPS initialization error at Server startup does not stop the EFT service. Instead, the service is started and listening for administrator connections, but the Sites are stopped so that you can connect, get diagnostics, disable FIPS mode, and so on.
- An administrator SSL certificate failure at Server startup does not stop the EFT service immediately. Instead, EFT starts, but does not accept SSL administrative connections. The administrator is able to login locally, get diagnostics, replace the certificate, and so on.
- An administrator SSL certificate failure after SSL FIPS mode switching does not stop the EFT service. Instead, EFT continues working, but does not accept SSL administrative connections. The administrator can connect to replace the certificate, and so on.

FIPS Mode Messages in the Administration Interface

EFT displays the following FIPS-related messages in the administration interface:



When EFT is in SSL or SSH FIPS mode, this message reports which Site protocols are FIPS-secured and which are not each time the administrator

explicitly starts the Site (for example, clicks **Go** or the Start button on the General tab of the Site).

The EFT is stopped: FIPS mode initialization error. All sites and protocols are disabled.

This warning message appears upon new administration connections if FIPS fails to initialize. FIPS can fail to initialize because EFT could not load the FIPS library or the library self-test failed. When this occurs, EFT is stopped and all Sites and protocols are disabled.

An error occurred while attempting to start EFT. FIPS mode initialization error; all sites and protocols have been disabled.

This message appears in the administration interface during Server start or restart when FIPS fails to initialize. FIPS can fail to initialize because EFT could not load the FIPS library or the library self-test failed. When this occurs, EFT is stopped and all Sites and protocols are disabled.

An error occurred while attempting to start Site '<SITE_NAME>. The SSL certificate provided for Site '<SITE_NAME>' has an improper key length. FIPS 140-2 mode requires keys between 1024 and 4096 bits (inclusive). Please choose a different certificate, or generate a new one that has at least 1024 but no more than 4096 bits in the public key.

Or, if other certificate error (forbidden algorithms, inconsistent private key, or invalid private key password):

An error occurred while attempting to start Site '<SITE_NAME>'. Could not load SSL certificate.

This message appears during Site start/restart if a Site uses SSL and its certificate does not meet FIPS requirements (for example, FIPS mode gets turned on and old certificate/key does not pass the FIPS test). The Site is stopped.

An error occurred while attempting to start Site '<SITE_NAME>. The SFTP key provided has an improper key length. FIPS 140-2 mode requires keys between 1024 and 4096 bits (inclusive). Please choose a different key, or generate a new one that has at least 1024 but no more than 4096 bits in the public key.

Or, if other certificate error (forbidden algorithms, inconsistent private key, or invalid private key password):

An error occurred while attempting to start Site '<SITE_NAME>'. Could not load SFTP certificate.

This message appears during Site start/restart if a Site uses SFTP and its key does not meet FIPS requirements (for example, FIPS mode gets turned on and old certificate/key does not pass the FIPS test). The Site is stopped.

The Site <SITE_NAME> is not started: [SSL certificate | SFTP key] is too weak and does not meet FIPS 140-2 requirements. Clients will not be able to connect to the Site.

Or, if other certificate error (forbidden algorithms, inconsistent private key, or invalid private key password):

The Site <SITE_NAME> is not started: could not load [SSL certificate | SFTP key]. Clients will not be able to connect to the Site.

This warning message appears during new administration interface connections if a Site uses SSL and its certificate does not meet FIPS requirements or uses SFTP and its key does not meet FIPS requirements (for example, FIPS mode gets turned on and old certificate/key does not pass the FIPS test). The Site is stopped.

EFT SSL certificate for remote administration is not an approved size (must be at least 1024 but no more than 4096 bits). Administrators will not be able to connect to EFT remotely.

Or, if other certificate error (forbidden algorithms, inconsistent private key, or invalid private key password):

EFT SSL certificate for remote administration is broken. Administrators will not be able to connect to EFT remotely.

This warning message is used in to notify all connected administration interfaces if the SSL certificate for remote administration does not meet FIPS requirements. Remote administration connections via SSL are not accepted.

EFT SSL certificate for remote administration is too weak and does not meet FIPS 140-2 requirements. Administrators will not be able to connect to EFT remotely.

Or, if other certificate error (forbidden algorithms, inconsistent private key, or invalid private key password):

EFT SSL certificate for remote administration is broken. Administrators will not be able to connect to EFT remotely.

This warning message is used during new administration interface connections if the SSL certificate for remote administration does not meet FIPS requirements. Remote administration connections via SSL are not accepted.

EFT [SSL | SSH] subsystem has entered FIPS mode. All new connections over [SSL | SSH] will use EFT's FIPS cryptographic libraries.

Or, if other certificate error (forbidden algorithms, inconsistent private key, or invalid private key password):

EFT [SSL | SSH] subsystem has exited FIPS mode. All new connections over [SSL | SSH] will use EFT's standard (non-FIPS) cryptographic libraries.

These informational messages appear in the administration interface to notify all connected administration interfaces when an administrator explicitly switches SSL or SSH FIPS mode or FIPS mode is disabled due to trial expiration.

FIPS Mode Events in the Event Log

EFT displays the following FIPS-related events in the Windows Event Log.

Globalscape EFT - FIPS [SSL|SSH] mode initialization error; all sites and protocols are disabled.

This error message appears in the Event Log upon the EFT service start or restart if FIPS fails to initialize. FIPS can fail to initialize because EFT could not load the FIPS library or the library self-test failed. When this occurs, EFT service is stopped and all Sites and protocols are disabled.

Globalscape EFT - FIPS mode initialization error for site "<SITE_NAME>": the specified [SFTP key|SSL certificate key] is not an approved size (must be at least 1024 but no more than 4096 bits). The site has not been started.

Or, if other certificate error (forbidden algorithms, inconsistent private key, or invalid private key password):

Globalscape EFT - FIPS mode initialization error for site "<SITE_NAME>": the specified [SFTP key|SSL certificate] is broken. The site has not been started.

This message appears during Site start/restart if a Site uses SSL and its certificate does not meet FIPS requirements or uses SFTP and its key does not meet FIPS requirements (for example, FIPS mode gets turned on and old certificate/key does not pass the FIPS test). The Site is stopped.

EFT SSL certificate for remote administration is not an approved size (must be at least 1024 but no more than 4096 bits). Administrators will not be able to connect to EFT remotely.

Or, if other certificate error (forbidden algorithms, inconsistent private key, or invalid private key password):

EFT SSL certificate for remote administration is broken. Administrators will not be able to connect to EFT remotely.

This warning message appears in the Event Log if the SSL certificate for remote administration does not meet FIPS requirements. Remote administration connections via SSL are not accepted.

EFT [SSL | SSH] subsystem has entered FIPS mode. All new connections over [SSL | SSH] will use EFT’s FIPS cryptographic libraries.

Or, if other certificate error (forbidden algorithms, inconsistent private key, or invalid private key password):

EFT [SSL | SSH] subsystem has exited FIPS mode. All new connections over [SSL | SSH] will use EFT’s standard (non-FIPS) cryptographic libraries.

This informational message appears in the Event Log when an administrator explicitly switches SSL or SSH FIPS mode or FIPS mode is disabled due to trial expiration.

Globalscape EFT - FIPS [SSL|SSH] mode initialized successfully; operating in compliance with FIPS 140-2.

This informational message appears in the Event Log every time the EFT service starts or restarts to report its successful FIPS mode initialization.

SFTP FIPS

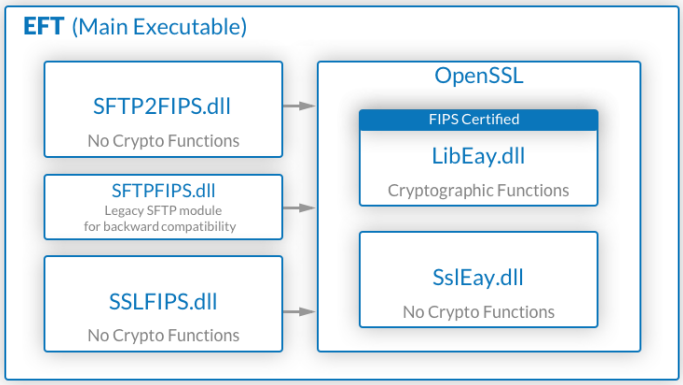
- If you are upgrading from 7.2.9 or 7.3.6 and later to version 7.4.x, and then upgrading to v8.x, you must export and convert your SFTP keys. Version 7.4.x only creates RSA keys in OpenSSH new format. (You can't generate DSS keys and save keys in SSH.com format.)
- After upgrading, the older ciphers and MACs will be removed automatically, without requiring any manual reconfiguration.
- Private keys from previous versions:
  - Non-FIPS mode
    - The private keys generated by previous versions should load just fine in non-FIPS mode. Both RSA and DSA and SSH.com formats are supported.
  - FIPS mode
    - FIPS mode does not support md5—only the new format keys are supported. The keys themselves are fine, it is the file format that is not supported. As a workaround, you can use a third-party tool like PuTTYGento convert your keys to the OpenSSH new format. If later you decide to go back to the older SFTP FIPS library, the new keys will not work and you will either have to use the previous keys or convert the new keys to the old format.
- After you enable or disable FIPS mode, you must restart the EFT server service.

EFT SFTP FIPS Mode

When placed in FIPS mode, all cryptographic functions required by the SFTP transport protocol are managed by the OpenSSL cryptographic library, which is FIPS certified and thus meets the requirements of organizations that require all cryptographic functions be FIPS certified. While many vendors claim compliance status, it is not the same as "certified," which means the module has undergone third-party laboratory testing. At a functional level, SFTP transport in EFT is based on a Windows port of a modified version of OpenSSH. Modifications were necessary because OpenSSH itself isn't a library, but rather a product. Also, many of the functions of OpenSSH aren't relevant to SFTP, such as command-line parsing, X-11 forwarding, and many others. Finally, OpenSSH doesn't support FIPS mode, and had to be modified following the principles applied by the Fedora FIPS patch that enables OpenSSH implementations on Fedora Linux to use OpenSSL in FIPS mode. When OpenSSH releases new versions, any beneficial changes (performance, security, etc.) can be merged into the SSH implementation in EFT.

Within the OpenSSH code, there are absolutely no cryptographic functions. All crypto is relegated to OpenSSL. In our implementation, OpenSSL consists of several libraries: **SslEay.dll**, which handles SSL network protocols, key pair loading and unloading, etc., **LibEay.dll**, which manages all cryptography and is FIPS certified, and **SSLFIPS.dll**, which acts as layer between EFT and OpenSSL. **SSLFIPS.dll**also does some key and network management, sans cryptography. OpenSSL is thus used both by SFTP and SSL/TLS-based protocols (that is, HTTPS, FTPS) in EFT.

Another benefit of this module is that the FIPS-certified cryptographic module is not tied to any particular OpenSSL version, which gives Globalscape the ability to keep current with OpenSSL releases, while conserving its FIPS-certified cryptographic functions, so long as the NIST certification remains current and valid.



SFTP Logging for Successful Connections:

- Level of logging in EFT.log should be set to DEBUG.
- The information should be semicolon separated
- Items recorded should be in the following order SFTP connection accepted: KEX algorithm = ; Host Key Algorithm = ; Cipher algorithm = ; MAC algorithm = ; Compression algorithm = ; ip address = ; connection ID =

SFTP Logging for Failed Connections:

- Level of logging in EFT.log should be set to INFO
- The information should be semicolon separated
- Items recorded should be in the following order SFTP connection failed; ip address=; connection ID=

SFTP Logging for Insecure Connections:

- Level of logging in EFT.log should be set to WARN.
- The information should be semicolon separated Items recorded should be in the following order Insecure SFTP connection accepted;

    - KEX algorithm = ; Host Key Algorithm = ; Cipher algorithm = ; MAC algorithm = ; Compression algorithm = ; ip address = ; connection ID =
- This should occur if the KEX algorithm used is one of the following: Diffie-Hellman-group1-sha1
- This should occur if the Cipher algorithm used is one of the following: arcfour
- This should occur if the MAC algorithm used is one of the following: hmac-md5; hmac-md5-96

SFTP Logging for Weak Connections:

- Level of logging in EFT.log should be set to WARN.
- The information should be semicolon separated.
- Items recorded should be in the following order:
    - Weak SFTP connection accepted; KEX algorithm = ; Host Key Algorithm = ; Cipher algorithm = ; MAC algorithm = ; Compression algorithm = ; ip address = ; connection ID =
    - Weak connections should occur if the:
        - KEX algorithm used is Diffie-Hellman-group-exchange-sha1
        - Cipher algorithm used is one of the following:
            - 3des-cbc
            - blowfish-cbc
            - cast128-cbc
        - MAC algorithm used is one of the following:
            - hmac-sha1
            - hmac-sha1-96

Ciphers and Algorithms

- In non-FIPS mode:
    - KEX:
        - diffie-hellman-group16-sha512
        - diffie-hellman-group14-sha256
        - diffie-hellman-group-exchange-sha256
        - diffie-hellman-group14-sha1
        - diffie-hellman-group-exchange-sha1
        - diffie-hellman-group1-sha1
    - MACs:

        - hmac-sha2-512
        - hmac-sha2-256
        - hmac-sha1
        - hmac-md5
        - hmac-sha1-96
        - hmac-md5-96
    - Ciphers:
        - aes-256-cbc
        - aes-256-ctr
        - 3des-cbc
        - aes-128-cbc
        - aes-128-ctr
- In FIPS mode the same as the above except hmac-md5 and hmac-md5-96

COM

- Due to FIPS requirements we can only generate keys on the server. This is the same as in SSL keypair generation. There is a new COM method "CreateSSHKeyRemotely" which works in the same way as previous version but creates key on the server machine, not where the COM is running. Older method "CreateSSHKey" still works, but it is always in non-FIPS mode.

Legacy BitVise implementation (Not available in v8.0.6 and later; removed Bitvise library)

- Advanced property
    - The new advanced property **UseLegacySFTP**allows switching to the old implementation. Setting it to 1 and restarting EFT will switch to legacy BitVise implementation.
- MACs, ciphers etc.
    - This setting only selects SFTP engine. Note that because BitVise implementation is quite old, it won't be able to load keys generated by the new version so they should either be recreated (or, for example, converted to one of the older formats using PuTTYgen).
- FIPS
    - You can switch BitVise to FIPS mode. However, this mode is obsolete and currently is not FIPS compliant.
- Switching back to the new version

- Switching back to the new implementation should not require any changes in configuration except when you are in FIPS mode. See the section above, "Private keys from previous versions" for details.

Remote Administration

The topics in this section describe how to enable and configure secure PNC in DMZ Gateway and EFT.

- Installing the Administration Interface Remotely
- Remote Administration of EFT
- Remote Administration FAQ
- Enabling REST API for Remote Administrator
- IP Access for Remote Administration
- Creating a Remote Connection
- Configure Remote Administration
- Starting and Stopping EFT Remotely
- Remote Administration through DMZ
- Introduction to Secure PNC
- Configuring Secure PNC
- Secure PNC Settings
- Secure PNC Logging

Installing the Administration Interface Remotely

When you install EFT, you also install the administration interface. After you have installed EFT and the administration interface on one computer, you can also install the administration interface on remote desktops. You do not need a separate license for each installation of the administration interface.

- The necessary DLL files are also installed and registered when you install the interface remotely, in case you plan to use the COM API remotely.
- For help using the COM API, refer to the online help for the COM API.

This procedure is for installing only the administration interface on a computer that is remote from EFT.

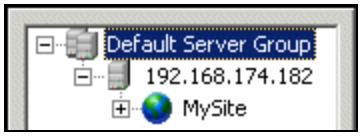
To install EFT and the administration interface on the same computer, refer to Installing the Server, Interface, and Modules.

To install the administration interface remotely

1. Close all unnecessary applications so that the installer can update system files without rebooting the computer.
2. Start the installer, and then click **Next**.
3. After installation components are loaded, the **Welcome** page appears.
4. Read the **Welcome**page, and then click **Next**. The **License Agreement** page appears.
5. Read the license agreement, and then click **I agree** to accept it. (Clicking **Cancel**aborts the installation.) The **Choose Components** page appears.
6. To install **only**the administration Interface, clear the **EFT Server** check box, and then click **Next**. The **Choose Install Location**page appears.
7. The default installation location appears in the **Destination Folder** box. Leave the default or click **Browse** to specify a different folder, and then click **Next**. The **Configuration data path**page appears.
8. Leave the default or click **Browse**to specify a different folder, and then click **Next**. The **Choose Start Menu Folder**page appears.
9. Keep the default shortcuts, specify an existing folder, or type a name for a new folder, and then click **Next**. The administration interface installs.
10. When installation is complete, click **Next**.
    - Leave the **Start the administration interface** check box selected so that you can configure a connection to the remote EFT next.

- If you want to create a desktop shortcut for the administration interface leave the **Create a desktop shortcut** check box selected.
- If you want to review the version history in your default text editor, select the **Show version history** check box.
- If you want to display the installation log, select the **Show installation log** check box.

11. Click **Finish**. The administration interface appears and the **EFT Server administrator Login** wizard appears.
12. Click **A remote computer**, then ensure the remote EFT's IP address appears in the drop-down list. If the remote EFT's IP address does not appear in the list, ensure you can connect to it from this computer and that remote administration is allowed on EFT. Otherwise, click **New**and configure the remote connection.
    - In the **Label**box, provide a name for the EFT to which you want to connect. You can call it anything you want; it has nothing to do with EFT's computer name. This name will appear in logs and reports.
    - In the **Host address**box, type the IP address of EFT computer.
    - In the **Port**box, type the port number used by EFT for remote connections.
13. Click **Next**. The **EFT Administrator Login**page appears.
14. Click the **Authentication**box and specify the type of authentication to use for this login. Future connections will default to the authentication type that you specify during this initial login, but you can choose a different type. Authentication types include:
    - **EFT Authentication**- Choose this option to log in with an EFT-specified administrator account.
    - **Integrated Windows Authentication** - Choose this option to log in with an Active Directory or local Windows account.
    - **Windows NET logon**- Choose this option to log in with a local Windows account.
15. In the **Username**and **Password** boxes, provide the login credentials that you created during installation, and then click **Connect**. The **Welcome**page appears.
    - If connection was not successful, verify the IP address and port on which EFT listens for connections, that remote administration is enabled on the server, and that SSL is properly configured, if used, on EFT.
    - If connection was successful, the remote Server appears in the tree.



Remote Administration

You can remotely administer EFT from any computer on which the administration interface is installed (with network access). If you are using SSL, you must create and/or assign an SSL certificate to use for connections. When you connect from a remote administration interface, an **SSL Certificate**dialog box appears in which you must accept the certificate to continue. If you reject the certificate, the User Connect Failed Event is triggered with the Event Reason of "Client SSL Certificate was rejected."

If you are not installing the administrative interface and plan to use the COM API for remote administration, refer to Remotely administering EFT Using the COM APIin the COM API reference.

Refer to FAQs About Remote Administration for several facts and caveats to consider regarding remote administration.

Refer to Remote administration via DMZ Gateway if you intend to allow EFT administration through DMZ Gateway.

Remote administration is not allowed after the trial expires if you do not activate the software.

If you are using SQL Express as your database, you may not be able to generate a report remotely, unless the connecting account is a trusted SQL Server connection (for example, if SQL Server and the remote computer are in the same domain, or if SQL Server is configured to allow "mixed authentication").

Remote Administration FAQ

EFT allows you to administer it remotely from any computer with network access. You can administer EFT with the administration interface (AI) or using the COM API. Below are several facts and caveats to consider regarding remote administration.

- If you are remotely connected to EFT via DMZ Gateway and make a change to the EFT<->DMZ Gateway settings, including disconnecting EFT from DMZ Gateway, the active session will not be affected. If/when you attempt to reconnect to EFT via DMZ Gateway, you will experience the effects of any changes.
- File browse operations are disabled. However, you can type a path that is relevant to the EFT computer (not the remote interface). For example, when you create a Command or a Monitor Folder Event Rule remotely, you can't click the folder icon and browse to the path of the file that you want to execute or the folder that you want to monitor on the EFT computer, but you can type the path. (No verification is done on the path that you type.) You are able to browse for a Settings Template folder, because you are browsing the VFS, not the physical folders.
- SSL and SSH certificates cannot be created or managed remotely. You are prohibited from creating certificates for EFT while remotely administering EFT because this action can create a security breach. Any certificates you create remain on the computer on which you created them, unless you take steps to deliver and associate these files with another computer. When you remotely connect to EFT Server, you will be prompted to Trust or Reject the server certificate.
- OpenPGP keys cannot be created or managed remotely.
- You do not need a separate license for each installation of the administration interface.
- When you install the AI remotely, SSL.DLL and SFTPCOMInterface.DLL are installed in **C:\Program Files\Common Files\Globalscape\SFTPCOMInterface** on the remote computer.
- Organizations complying with the PCI DSS are required to use SSL for remote administration. If you attempt to allow remote administration on a high security-enabled Site without SSL, a message warns you that this setting violates PCI DSS, and allows you to continue with reason or disable the feature.
- When the trial period has expired, all remote connections are disallowed.
- You cannot activate the server or modules through a remote installation of the administration interface.

- You cannot configure remote administration remotely.
- You must configure the local connection before you can configure a remote connection.
- When you are upgrading, remember to upgrade any remote installations of the administration interface to the same version.
- For remote Active Directory connections, the connecting account must have access to the computer on which EFT is installed.
- You can select AD accounts when performing remote administration as long as the administration interface and EFT are in the same domain or working across trusted domains.
- You can login using the EFT computer's local administrator credentials from a command line or a Windows shortcut, using the EFT listening IP address and port.
- You should restrict remote administration to one or more known static IP addresses.
- By default, all IP addresses are granted remote access to EFT. EFT allows you to grant access to only one specific IP address or a range of IP addresses, or deny access to one specific address or a range of addresses.
- For command-line login, the EFT listening IP address must be set to a specific IP address, not **All Incoming**. Remote administration must be configured and EFT must be in the same domain as the computer from which you are attempting to log in.
- Before attempting to connect to a remote EFT, first be sure that the remote EFT service is running, and that it allows remote administration.
- If you are logged in to EFT remotely, your username and password are passed to the Windows System Services on the computer running EFT. The account that you log on with must have administrative rights to make any changes to the Globalscape EFT service running on that computer.
- If you are using SQL Express as your database, you may not be able to generate a report remotely, unless the connecting account is a trusted SQL Server connection (for example, if SQL Server and the remote computer are in the same domain, or if SQL Server is configured to allow "mixed authentication.")
- When objects are created, added, removed, modified, enabled, disabled, started, or stopped remotely, the action is logged to the database.
- The EFT variable for remote EFT connections is %CONNECTION.REMOTE_IP%.
- If you are unable to connect to a remote server, verify that the remote server is configured to allow remote administration, and that you have provided the correct IP address, port, and login information.

What you can't do remotely:

- File browse operations are disabled. However, you can type a path that is relevant to the EFT computer (not the remote interface). For example, when you create a Command or a Monitor Folder Event Rule remotely, you can't click the folder icon and browse to the path of the file that you want to execute or the folder that you want to monitor on the EFT computer, but you can type the path. (No verification is done on the path that you type.)
- SSL and SSH certificates cannot be created or managed remotely.

Before you can connect from the remote administration interface, you must:

1. Configure the Server. You must do this locally, on EFT computer.
2. Configure remote administration, as described below.

If you have configured remote administration, but are unable to connect, one or more of the following could be preventing the connection:

- The IP address of the computer on which you are attempting to connect to EFT is listed in the Remote administration Ban IP list.
- Your SSL certificate is expired or invalid.
- The **Allow remote administration** check box has been cleared.
- The remote administration port value has changed.
- EFT's IP address has changed since the last login.
- The firewall settings of the computer on which EFT is installed are blocking the connection.
- There is a version mismatch between your administration interface and the EFT service that you are trying to administer.
- The account with which you are attempting the remote connection does not have access permission to EFT.
- Network errors

The following topics describe:

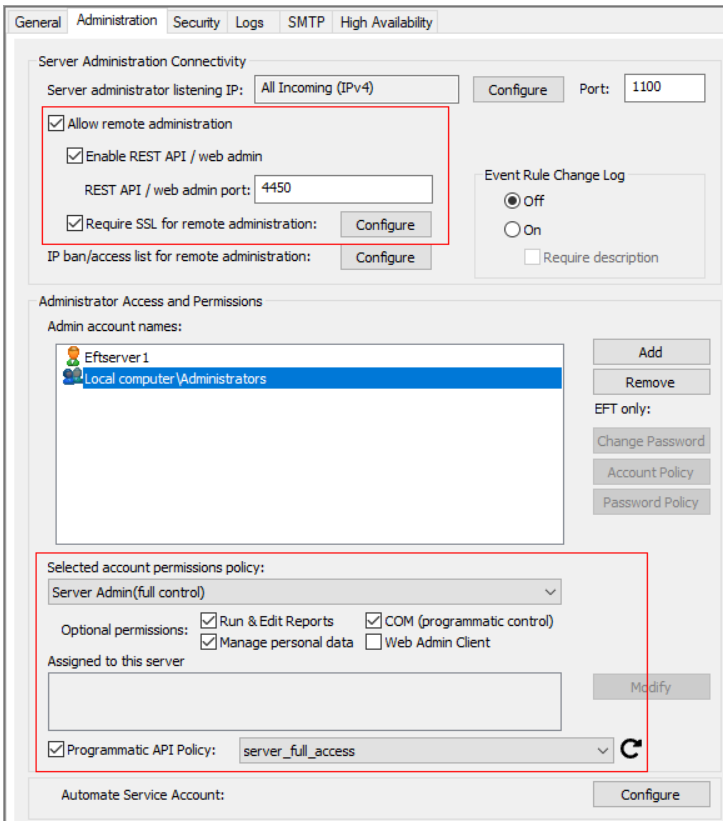
- How to configure EFT for remote administration
- How to configure the remote administration interface
- FAQs About Remote administration

Enabling REST API for Remote Administration

To use the EFT REST API to administer EFT remotely, you first must enable REST API in the EFT administration interface.

To enable REST API for remote administration

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node that you want to manage.
3. In the right pane, click the **Administration**tab.



4. Select the **Allow remote administration** check box.
5. Select the **Enable REST API /web admin** check box.
6. Specify the **REST API /web admin port**. The default is 4450.
7. (Optional) Select the **Require SSL for remote administration** check box, then specify the SSL certificate to use.

8. At the bottom of the tab, select the **Programmatic API Policy**check box, and then select the **server_full_access** permission.

   > **NOTE:** When the **Web Admin Client** check box is selected, the Programmatic Policy automatically changes to "use account permission policy."

9. Click **Apply**to save the changes on EFT.

Refer to Configuring REST Permission Roles for details of the **Programmatic API Policy** settings and configuring REST permissions.

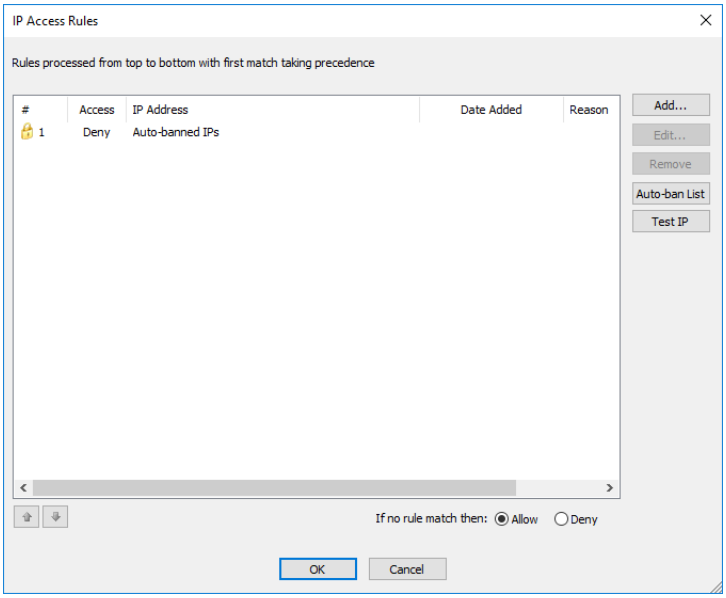
IP Access Rules for Remote Administration

By default, all IP addresses are granted remote access to EFT. EFT allows you to grant remote administrationaccess to only one specific IP address or a range of IP addresses, or deny access to one specific address or a range of addresses. Refer to Controlling Access to the Site by IP Address for details of banning IP addresses.

To grant/deny access by IP address

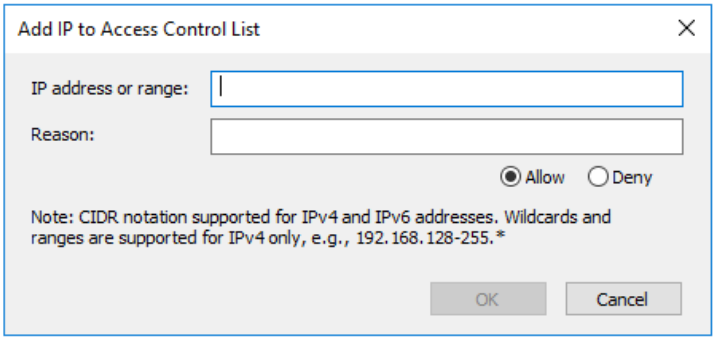
1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node that you want to configure.
3. In the right pane, click the **Administration**tab.
4. Select the **Allow remote administration** check box.
5. Next to **IP ban/access list for remote administration**, click **Configure**.

   The **IP Access Rules** dialog box appears. The default configuration is to deny access to automatically banned IP addresses. By default, if no rule matches an IP address, then the IP is allowed.



   - Click **Deny** if you want to exclude all IP addresses that are not explicitly defined in the Rules list.

   To add an IP address to the rules, click **Add**. The **Add IP to Access Control List** dialog box appears.

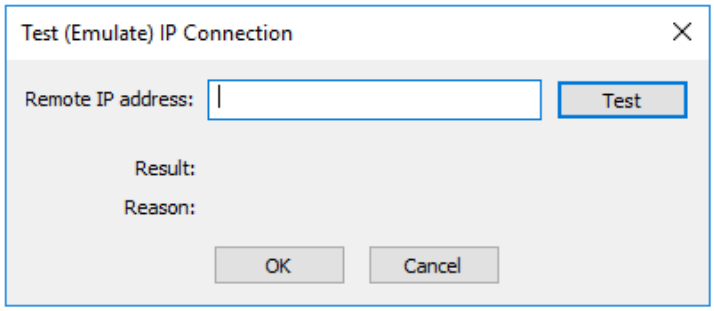


a. Specify the IP address or mask.
b. Provide a reason for allowing or denying the IP access. (optional)
c. Click whether to **Allow**or **Deny** the address.
d. Click **OK**. CIDR notation is supported for IPv4 addresses (for example, 192.168.29.0/24) and literal IPv6 addresses (for example, 001:cdba:9abc:5678::/64).

To remove a rule, click it in the list, and then click **Remove**. A confirmation prompt appears. Click **Yes**. (You cannot remove the default rule.)

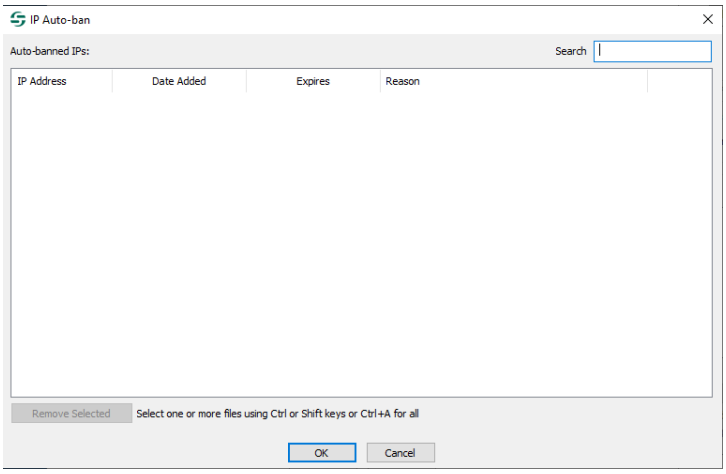
To edit a rule, click it in the list, and then click **Edit**. The **Add IP to Access Control List**dialog box appears for you to edit the address. Click **OK**to save your edits.

To test whether an IP address is banned or allowed, click **Test IP**. The **Test IP Connection**dialog box appears.



- Provide an IP address to test, and then click **Test**. The **Result**(Allowed or Denied) and the **Reason**the IP is allowed or denied appear in the dialog box. Click **OK** to close the dialog box.

To view the list of banned IP addresses, click **Autoban List**. The **IP Auto-ban** dialog box appears.



NOTE: Temporarily banned IPs are not stored in the database. They are kept in runtime memory. They are also node-specific.

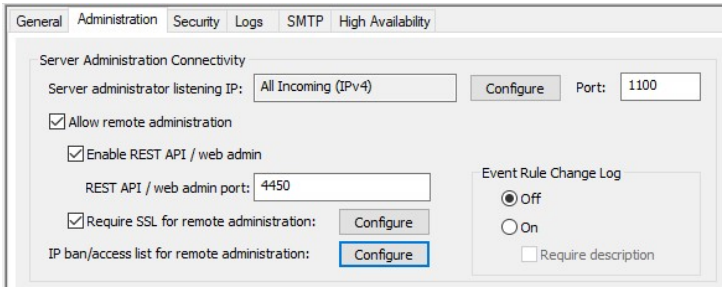
- The **IP Address**column lists the banned IP addresses.
- The **Date Added**column displays the date and time the IP address was automatically banned, in MM/DD/YYYY hh:mm:ss AM/PM format.
- The **Reason**column displays the reason the IP address was automatically banned (for example, DoS/Flood prevention temporary ban, DoS/Flood prevention permanent ban, Invalid password attempts exceeded, Invalid username attempts exceeded, Too many consecutive invalid commands).
- To find an IP address in the auto-ban list, type it in the **Search** box.
- To sort the auto-ban list, click a column header.
- To remove an IP address from the auto-ban list, click it, and then click **Remove Selected**.

6. Click **OK** to close the dialog boxes.
7. Click **Apply**to save the changes on EFT.

REST API Support via DMZ Gateway

EFT enables REST API support via DMZ Gateway so that you can maintain your current security posture. A Site admin or Server admin can add the REST API protocol to the DMZ Gateway. Whether added for one or more sites, the inbound connection to the specified IP:port will be routed to the REST API listener (a single, server-side listener).

REST API via the DMZ Gateway requires that the **REST API/ web admin** check box is selected on the EFT Server > **Administration** tab, under the **Allow remote administration** check box.



- You must have at least one whitelisted IP specified under IP Access Rules for Remote Administration.

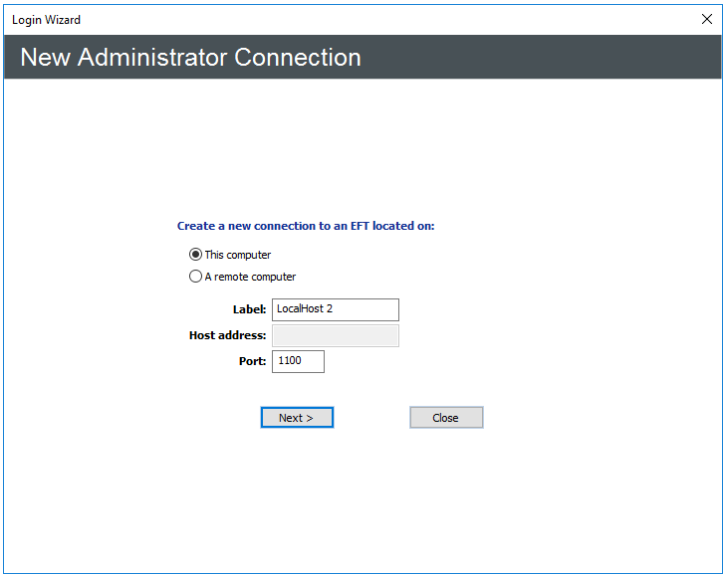
Refer to Enabling REST API for Remote Administration for more information.

Creating a Remote Connection

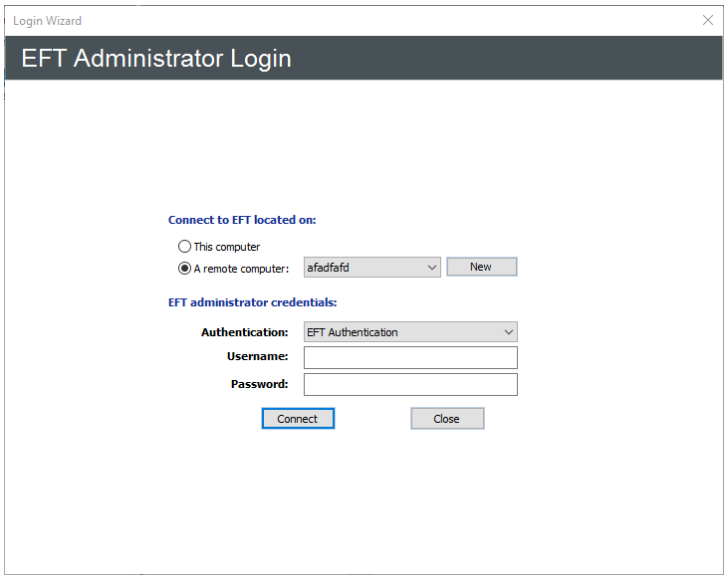
After you have configured a local connection to EFT, you can create a remote connection.

To create a remote EFT administrator connection

1. On the main menu click **File >New Server**. The **New administrator Connection** page appears.



2. Be sure that the remote Server service is running, and that it allows remote administration. Then:
    a. Click **A remote computer**.
    b. In the **Label**box, provide a name for the remote Server.
    c. In the **Host address**box, provide the IP address at which the remote Server allows connections.
    d. In the **Port**box, provide the port through which the remote Server allows connections.
3. Click **Next**. The **Login** page appears.



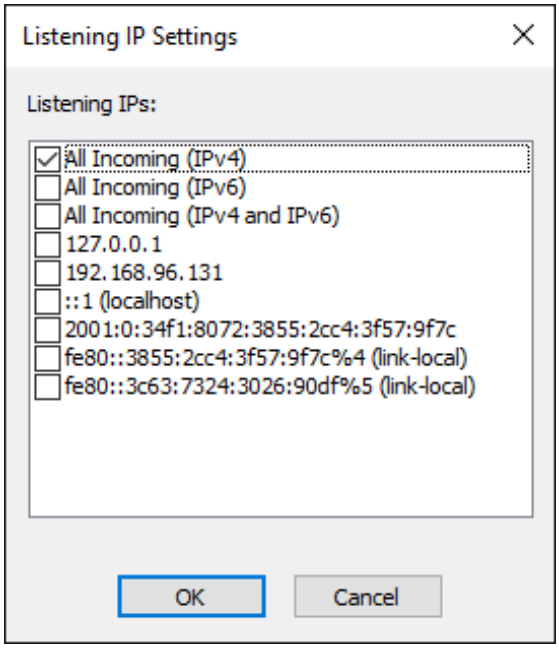
4. Click the **Authentication**box and specify the type of authentication to use for this login. Future connections will default to the authentication type that you specify during this initial login, but you can choose a different type. Authentication types include:
    - **EFT Authentication**- Choose this option to log in with an EFT-specified administrator account, such as the one you created during installation.
    - **Integrated Windows Authentication** - Choose this option to log in as the currently logged on user (Integrated Windows Authentication). .
    - **Windows Authentication**- Choose this option to log in using a specific Windows account.
5. If you specified **EFT Server Authentication** or **Windows Authentication**, in the **Username**and **Password** boxes, provide the login credentials that you created during installation. The **Welcome** page appears. Because you have not yet activated the software, the "Free Trial" reminders appear. After you activate, you will not see this prompt.
6. Do one of the following:
    - If you are evaluating the software or just do not want to activate yet, click **Start Trial**, then follow the procedures in Configuring EFT.
    - If you have purchased a license, click **Activate Now**, then follow the procedures for activating the software.
7. Click **Next**. The **Server Setup** wizard **Welcome** page appears.
8. If you are restoring from a backup, click **Restore from Backup**, then refer to Backing Up or Restoring Server Configuration for the procedure. Otherwise, continue to the next step.

9. If you are not restoring from a backup, click **Next**. The **FIPS Options** page appears.

   When you enable FIPS mode, the ciphers, keys, and hash lengths and types that are not FIPS approved are not available. If a FIPS-approved state cannot be achieved when FIPS is enabled, the EFT service is stopped and an error is written to the Windows Event Log.

   - To use FIPS for SFTP (SSH2), select the **Enable FIPS for SFTP** check box.
   - To use FIPS for SSL, select the **Enable FIPS for SSL** check box.
   - A confirmation prompt appears when you select either check box. When you enable FIPS, the EFT service must be restarted. Click **OK** to continue with FIPS enabled or click **Cancel**if you do not want to use FIPS and restart the EFT service.

10. Click **Next**. The **Remote administration**page appears.
11. Because you are configuring a remote administrator connection, ensure that the **Allow remote administration** check box is selected.
12. Specify the **Listening IPs**.
    a. Click **Configure**to specify one or more IP addresses. The **Listening IP Settings** dialog box appears.



    b. **All Incoming (IPv4)** is selected by default. Select the check boxes for addresses that you want to allow; clear the check boxes for the addresses that you do not want to allow, and then click **OK**.

13. Specify the **Listening port**. (For security best practices and compliance with the PCI DSS, specify a port other than the default of 1100.)
14. Click **Next**. The **Secure Remote administration**page appears.
15. Administrator account credentials are transmitted in plain text unless SSL is enabled. Organizations complying with the PCI DSS are required to use SSL for remote administration. To enable secure remote administration, select the **Use SSL for secure remote administration** check box, and then click **Next**. The **SSL Certificate Options**page appears.
16. Do one of the following:
    - In the **Certificate**and **Private Key** boxes, click the folder icon to browse for the private key pair files.
    - Click **Create certificate** to create one. Refer to SSL Certificate-Based Login, Creating Certificates, Importing a Certificate into the Trusted Certificate Database for information regarding certificates.
17. Click **Next**. The **Auditing and Reporting**page appears.
18. If you are using Auditing and Reporting, select the **Enable auditing** check box, then provide the information required to connect to the ARM database as described below. If you are not using Auditing and Reporting, skip to the next step. (Auditing and reporting is a requirement of the PCI DSS.)
    a. In the **Database type** area, specify whether you are using **SQL Server** or **Oracle**for the auditing database.
    b. In the **Host[\Instance Name]** box, type EFT name or IP address.

       If you are using SQL Server as the Auditing Database, **\InstanceName** corresponds to SQL Server's notion of named instances, a feature that allows a given computer to run multiple instances of the SQL Server Database Service. For more information, refer to http://msdn2.microsoft.com/en-us/library/ms165614.aspx

    c. In the **Authentication**box, specify the type of authentication used by the database, either **Windows Authentication**or **SQL Server Authentication**.
       - If you choose **SQL Server Authentication**, you must also specify the "sa" username and password. In the **Username** and **Password** boxes, type the username and password used to connect to the database (***not***the EFT credentials).
    d. In the **Database Name** box, type the name of the database.
    e. In the **Audit failure notification email address** box, type the email address to which EFT is to send database connection error notifications. You can add as many email addresses as needed; separate the addresses with a comma or semicolon. EFT uses its global SMTP email settings from the

SMTP Configuration to send the emails. You will configure those settings on the next page.

f. In the **In case of audit database error** area, specify an Action for EFT to take if there is an error with the database. To stop recording data, select **Stop auditing**. To continue recording data to a file, select **Audit to folder**, and specify the location for the log file.

   UNC paths are supported. The Globalscape Server service must run on a computer that has access to the network share, and the full UNC path must be used, that is: \\xcvd.forest.intranet.xc\Common_Files, **not** G:\Common.

19. Click **Next**. The specify **SMTP Server Settings**page appears.
20. In the **From email address** box, specify the email address for email notifications (such as those triggered by Event Rules). This is the address that appears in the **From** box of emails sent by EFT. For example, type `noreply@serverhost.com`.
    - The email address is validated when you click **OK**. If the email address contains invalid characters or does not contain the @, an error message appears. Click **OK**to dismiss the error message, then correct the address.
21. In the **SMTP host address** boxes, specify the SMTP server host address and port.
22. If the **Use SMTP server authentication**, select the check box and provide the **Username** and **Password**.
23. Click **Next**. Server Setup is complete.

    You are offered the option of continuing to the Site Setup wizard, or quitting the wizard, saving EFT settings, and configuring the Site(s) later. You must configure at least one Site to service inbound connections to EFT.

24. Click an option, then click **Finish**. If you chose FIPS mode for SSL and/or SSH, prompts appear explaining that EFT has entered FIPS mode. Click **OK**to dismiss the prompts.
25. If you chose **Run the Site Setup wizard now**, the Site Setup wizard **Welcome** page appears.
26. Refer to Creating a Site for the procedure for configuring the Site. The procedure differs depending on the user authentication type you choose.

Related Topics

- Connection Problems
- Creating a Remote Connection
- Creating a Site

Configure Remote Administration

To configure EFT for remote administration

1. Launch the administration interface on EFT computer and connect to EFT you want to configure for remote administration. (You cannot setup remote administration remotely.)
2. In the right pane, click the **Administration**tab.
3. In the **Server administrator listening IP** box, specify the IP address that is allowed to connect remotely. You can select a specific IP address that is defined on the computer on which EFT is installed or **All Incoming** IP addresses. (For command-line login, the EFT administrator listening IP address must be set to a specific IP address, not *All Incoming*.)
    - For remote administration through DMZ Gateway, be sure to use the IP address of DMZ Gateway, not EFT.
4. In the **Port**box, specify the port on which EFT listens for connections. The default port is 1100. For security, you should use a different port other than the default.
5. Select the **Allow remote administration** check box. A warning message appears advising you to connect over SSL for more secure administration.

    If you attempt to allow remote administration on a high security-enabled Site, a message appears to warn you that this setting violates PCI DSS, and allows you to continue with reason or disable the feature.

6. Click **Yes**to set up secure administration or **No**to administer the server over a clear (not secure) connection.
7. To require SSL for remote connections, click the **Require SSL for remote administration**check box, and then click **Configure**. Refer to Assigning a Certificate for details of configuring SSL.
8. Click **Apply**to save the changes on EFT.
9. Close the administration interface. Make sure that the EFT service is still running, then configure the remote administration interface using the procedure below.

To configure the remote administration interface

1. Launch the administration interface on the remote computer.
2. Click the **Server**tab.
3. Click the group to which you want to add the remote server. (Click **File > New Group** if you need to define a new group.)

4. Right-click the group, then click **New Server**. The **Login** wizard **New Administrator Connection** page appears.
5. Click **A remote computer**.
6. In the **Label**box, type the name of EFT to which you want to connect. You can call it anything you want; it has nothing to do with EFT's computer name.
7. In the **Host address**box, type the IP address of EFT computer.
8. In the **Port**box, type the port number used by EFT.
9. Click **Next**. The **EFT Administrator Login**page appears.
10. Click **A remote computer**, then click its name (the label you gave EFT in step 6) in the box.
11. In the **EFT administrator credentials** area, provide your **Username**and **Password**, and then click **Connect**.

    If SSL is required for remote administration, a **Server Certificate**dialog box appears.

12. Accept or reject the SSL certificate from the remote EFT by clicking **Trust Once** (just for this session), **Trust Always**(for this and future connections, provided the SSL certificate does not change), or **Reject** (do not accept the certificate and do not connect to the server). (To undo a trust-always certificate, delete the appropriate trusted certificate file(s), stored in the **%AppData%**directory as **Cert_for_<ip>.crt**.)
    - If connection was successful, the remote Server appears in the tree.
    - If connection was not successful, verify the IP address and port on which EFT listens for connections, and ensure that SSL is properly configured on EFT, if used.

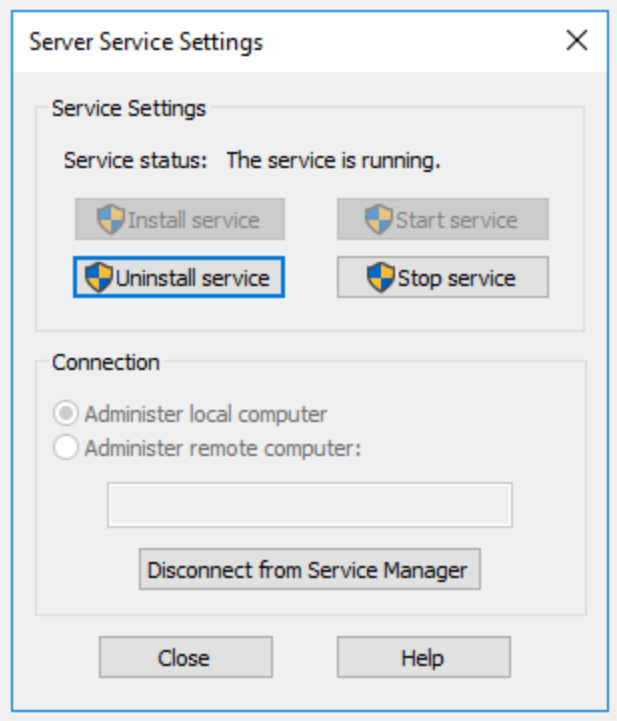
Starting and Stopping EFT Remotely

If you are logged in to EFT remotely, your username and password are passed on to the Windows System Services on the computer running EFT. The account you log on with must have administrative rights to make any changes to the Globalscape EFT service running on that computer.

When you stop the service, EFT breaks all existing connections and waits until all socket threads die. The service can terminate when Timer Event processing is still in progress. The triggering of Monitor Folder and Timer Event Rules occurs almost simultaneously and is controlled by the operating system, not by EFT. Refer to Event Rule Order of Execution for more information.

To start or stop EFT remotely

1. In the administration interface, click **Edit > Server Service Settings**. The **Server Service Settings** dialog box appears.



2. In the **Connection**area, select **Administer remote computer**.
3. In the text box, type or paste the IP address of the server you want to administer.
4. Click **Connect to Service Manager**.
5. Click **Start service** (or **Stop service**) and close the **Server Service Settings** dialog box.

Related Topic

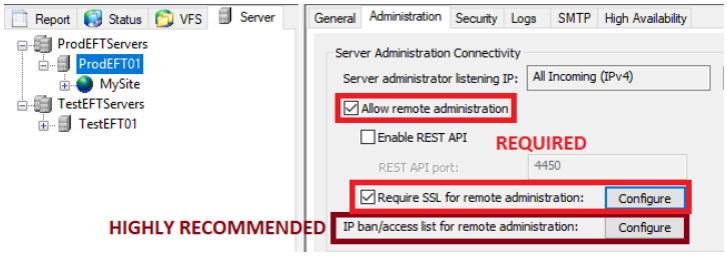
- Starting and Stopping EFT

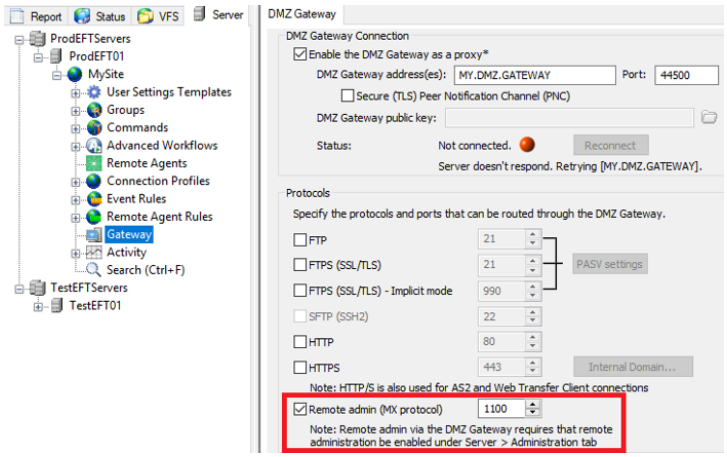
Remote Administration through DMZ Gateway

EFT shares its Site-level manual IP access list and permanent auto-ban IP (not temporary auto-ban) list to DMZ Gateway so that it can block IP addresses before reaching EFT.

Now that remote administration can be routed through DMZ Gateway, we allow EFT to transmit the remote administration manual IP access list to DMZ Gateway for the same purpose. For a client to perform remote administration through DMZ Gateway, its IP must pass both the Site-level and remote administration IP access validation. Note that the remote administration auto-ban feature in EFT is hardcoded to ban IP addresses temporarily, NOT permanently. Therefore, this auto ban list is not communicated to DMZ Gateway and rather it is enforced by EFT itself.

For customers with a new version of EFT supporting the remote administration through DMZ Gateway feature, and with an older DMZ Gateway, they can still do remote administration through DMZ Gateway, but only Site-level manual and Site-level permanent auto-ban IP access lists will be enforced at the DMZ Gateway. Remote administration IP access lists will be enforced only by EFT.





Notes to consider:

1. To enable remote administration through DMZ Gateway, you'll need to enable remote administration in the EFT administration interface at the Server level and select the **Require SSL for remote administration** check box.
2. The Site and remote administration **IP access/ban lists** in EFT are combined at DMZ Gateway. If there is a conflict, e.g., the remote administration block list allows an IP address that is blocked at the Site level, then the IP address will be blocked (least privileges assignment).
3. If EFT automatically bans an IP address temporarily (as result of DoS/Flooding or other trigger), that IP address will ***not***be shared with the DMZ Gateway. The administration access will still be blocked, but at EFT, not DMZ Gateway. The administrator can manually add those IP addresses to the permanent ban list, which will propagate to DMZ Gateway.
4. EFT can work with older DMZ Gateway versions (v<3.5) and still allow remote administration; however, when connected to an older DMZ Gateway, any IP address in the administration access/ban list will NOT be shared with the DMZ Gateway, as the older versions do not support receiving the administration IP access/ban list. Again, EFT will still block the connection, but DMZ Gateway will not.
5. If you are remotely connected to EFT via DMZ Gateway and make a change to the EFT<->DMZ Gateway settings, including disconnecting EFT from DMZ Gateway, the active session will not be affected. If/when you attempt to reconnect to EFT via DMZ Gateway, you will experience the effects of any changes.

Introduction to Secure PNC

EFT administrators might want to administer EFT from a location external to the network by connecting through the DMZ Gateway instead of having to RDP in to the server. The Peer Notification Channel (PNC) between DMZ Gateway and EFT is not, itself, encrypted. Instead, the PNC leverages the encryption provided by the secure protocols (for example, FTPS, SFTP, HTTPS) in EFT. This inherently encrypts the traffic traversing through the DMZ Gateway and traffic will remain encrypted until it reaches EFT. In this way, the PNC is not susceptible to man-in-the-middle attacks and does not present any real world security risks as long as EFT is using secure protocols.

If you want to further enhance the security of the data passing through DMZ Gateway, you can enable secure PNC settings in DMZ Gateway and EFT. The secure PNC settings will reduce false positives for security scans and reduce the attack vector.

Configuring Secure PNC

Secure PNC will work using a self-signed certificate created with OpenSSL or one created from EFT. Depending on the certificate used, different configuration steps must be taken, as described below.

There are two ways of authenticating the communication between EFT and DMZ:

- Non-mutual authentication
  - EFT will blindly trust the DMZ Gateway certificate and DMZ Gateway will blindly trust the EFT certificate.
- Mutual authentication
  - EFT will only trust that single certificate and DMZ Gateway will require EFT to provide a client certificate during the SSL handshake and it must match the DMZ Gateway server's certificate trust store.

Configuring Secure PNC using a Self-Signed Certificate

To configure Secure PNC using a self-signed certificate

1. Stop the DMZ Gateway Service.
2. On the DMZ Gateway server, open a command prompt and navigate to **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin**.
3. Type the following command to create a self-signed certificate:

```
keytool -genkeypair -alias test -keyalg RSA -validity
        365 -keystore keystore.jks
```

4. Enter a keystore password (for example, test123!).
5. Follow the prompts for creating the self-signed certificate.
6. Follow the steps for Non-Mutual Authentication between EFT and DMZ or steps for Mutual Authentication between EFT and DMZ, above.

Configuring Secure PNC using an EFT Certificate

This certificate will be used later for Mutual Authentication with the DMZ Gateway server.

The procedure below requires OpenSSL to convert the public and private EFT keys into a .p12 format and Java's keytool to create a keystore.jks file.

***To* configure Secure PNC using an EFT-generated certificate**

1. Install EFT Server.
2. Launch the EFT administration interface.
3. Create the default Site with SSL enabled
4. Create a new SSL Certificate, making sure the certificate password is at least 6 characters long. (This certificate will not be associated with any EFT Site; this is used instead of creating a certificate using OpenSSL.)
5. Install OpenSSL (use version 1.0.2 or later).
6. Copy the private and public certificates from Step 4 into the bin directory of OpenSSL (this makes it easier), **C:\OpenSSL-Win32\bin**
7. Using OpenSSL, run the following (update where necessary):

   ```
   openssl pkcs12 -export -in [filename-certificate]
          -inkey [filename-key] -name [host] -out [filename-new-
   PKCS-12.p12]
   ```

   (Refer to https://www.wowza.com/docs/how-to-import-an-existing-ssl-certificate-and-private-keyfor information about how to convert the certificate and private key to PKCS 12 (.p12).)
8. If you see a warning related to "can't open config file," then cancel the entry from Step 7 and run this command instead:

   ```
   set OPENSSL_CONF=[path-to-OpenSSL-install-
   dir]\bin\openssl.cfg
          (i.e. set OPENSSL_CONF=c:\OpenSSL-Win32\bin\openssl.cfg)
   ```
9. When prompted for a passphrase, enter the certificate password you used when this certificate was created in EFT.
10. On the DMZ Gateway server, use Windows File Explorer to navigate to the DMZ Gateway installer's **/bin/**path, e.g., **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin**.
11. Copy the **.p12** certificate from Step 7 into the DMZ Gateway installer's **/bin/** path in the previous step. (This makes it easier to create the keystore.jks file.)
12. Open Command Prompt to the DMZ Gateway installer's **/bin/**path and enter the following command (update where appropriate):

    ```
    keytool -importkeystore -deststorepass [password]
    -destkeystore [filename-new-keystore.jks]
    -srckeystore [filename-new-PKCS-12.p12]
    -srcstoretype PKCS12
    ```

(where [password] is the original password set when the private key was created in Step 4)

You have successfully created a **keystore.jks**file that can be used to use non-mutual authentication between EFT and DMZ, described below.

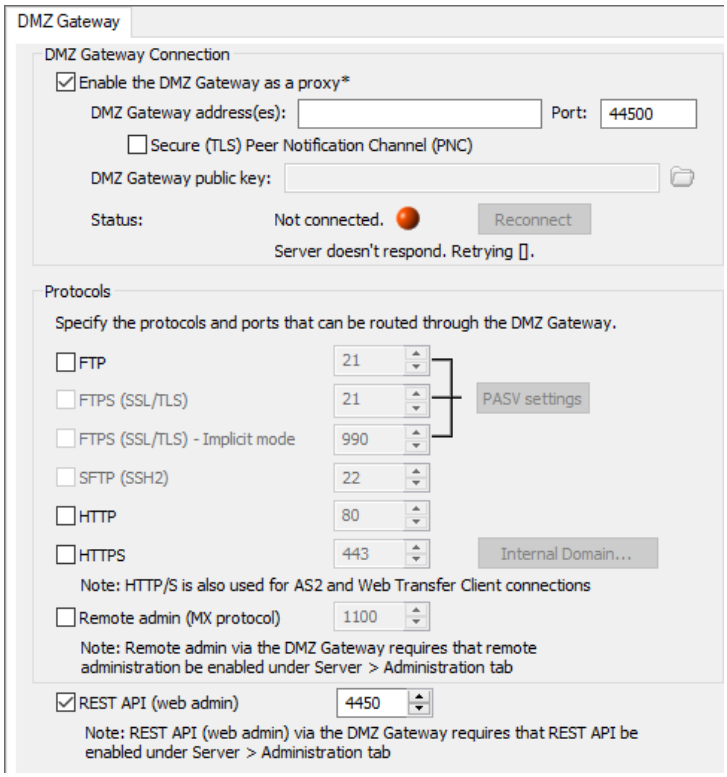
Non-Mutual Authentication setup

1. For simplicity, you can copy the **keystore.jks f**ile that was created above to a path that is easily accessible (for example, **C:\keystore\keystore.jks**), because you will have to paste the path in the DMZ Gateway xml configuration file.
2. Open Notepad or another text editor as an administrator.
3. Open the DMZ Gateway configuration file (gwconfig.xml), located in **C:\Program Files\GlobalSCAPE\DMZ Gateway.**

   (If the configuration file does not exist, start or restart the service and the file will be created.)
4. Set the <**SecurePNCEnabled**> value to "true."
5. Set the <**PNCKeyStorePath**> to the path where the **keystore.jks**is located (for example, **C:\keystore\keystore.jks**)

   > **NOTE:** You must enter the proper XML format for these values otherwise the service will not start, e.g., `<PNCKeyStorePath>c:\keystore\keystore.jks</PNCKeystorePath>`
6. Enter the store passphrase; because we imported the certificate into the keystore, this will default to the password created in EFT's certificate creation.
7. Save the XML file.
8. Close the XML file.
9. Start the DMZ Gateway service.
10. Re-open the XML file and verify the passphrase is now encrypted (this will also help confirm DMZ picked up the changes).

    NOTE If you are making any changes to the XML file, make sure the DMZ Gateway service has been stopped **prior to** making the changes.
11. To verify EFT detects that DMZ is configured, launch the EFT administration interface.



12. Click the **DMZ Gateway**tab.
13. Enable DMZ Gateway and provide the IP address of the DMZ Gateway, but do not select the **Secure TLS/PNC**check box.
14. Click **Apply**.
15. Verify that the EFT administration interface receives an error message.
16. Click **OK** on the error message.
17. Select the **Secure (TLS) Peer Notification Channel (PNC)** check box.
18. Click **Apply**.

DMZ Gateway and EFT are now configured with PNC SSL+ non-mutual authentication.

Mutual Authentication Setup

1. Copy the EFT SSL Site certificate (certificate associated with the SSL certificate settings) into the DMZ bin directory, e.g., **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin**.
2. Stop the DMZ Gateway Service.
3. To import EFT's SSL site certificate into the DMZ's Java truststore, open a command prompt and navigate to **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin**.
4. Run the following command:

```
keytool -import -alias EftClientCert -file "MySite
        Certificate.crt" -keystore truststore.jks
```

5. When prompted, enter the password of the keystore (not the password of the EFT site's certificate).
6. When prompted, type yes and press ENTER to trust the certificate.
7. Copy **truststore.jks**from the **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin** and place it in an easily accessible location (for example, **C:\keystore\truststore.jks**).
8. Open Notepad (or another text editor) as an administrator.
9. In Notepad, open the DMZ Gateway configuration (XML) file: **C:\Program Files\GlobalSCAPE\DMZ Gateway\gwconfig.xml**
10. Add the **PNCTrustStorePath**value, e.g., `<PNCTrustStorePath>c:\keystore\truststore.jks</PNCTrustStorePath>`.
11. Save and close the XML file.
12. To export the truststore certificate, open a command prompt and navigate to **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin**.
13. Run the following command:

    ```
    keytool -export -alias test -keystore keystore.jks
            -rfc -file DMZGatewayCert.cer
    ```

14. If you don't recall the alias that you used, type the following command:

    ```
    keytool -list -v -keystore keystore.jks
    ```

    (This will give you the alias of your keystore)
15. When prompted enter the password of the keystore.
16. Copy the newly created certificate to EFT.
17. Log in to the EFT administration interface, and click the **DMZ Gateway** tab.
18. In the **DMZ Gateway public key**section, click the folder and navigate to the certificate that was copied to EFT.
19. Click **Apply**.

    Remote administration via the DMZ Gateway requires that remote administration be enabled on the **Server > administration** tab.

DMZ Gateway and EFT are now configured with Secure PNC with mutual authentication

Secure PNC Logging

In most cases, you can inspect the **DMZGatewayServer.log** for log entries of interest.

For more detailed SSL logging, edit the **DMZGatewayServerService.conf** file by uncommenting this line and restarting the DMZ Gateway server service:

```
#wrapper.java.additional.6=-Djavax.net.debug=ssl:handshake:data
```

This will print each SSL handshake message to the **DMZGatewayServerService.log** file.

Other options for javax.net.debug can be found in https://docs.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html#Debug.

It is generally easier to troubleshoot secure PNC communication issues from the perspective of the DMZ Gateway due to the detailed logging that Java offers through that **javax.net.debug** option.

You can also use Wireshark to observe the communication from another perspective and/or to validate that encryption is actually being used on the channel.

Secure PNC Settings

After installing the DMZ Gateway, open **gwconfig.xml**in the root install folder with a text editor like Notepad. It should have the settings below for each DMZ Gateway profile.

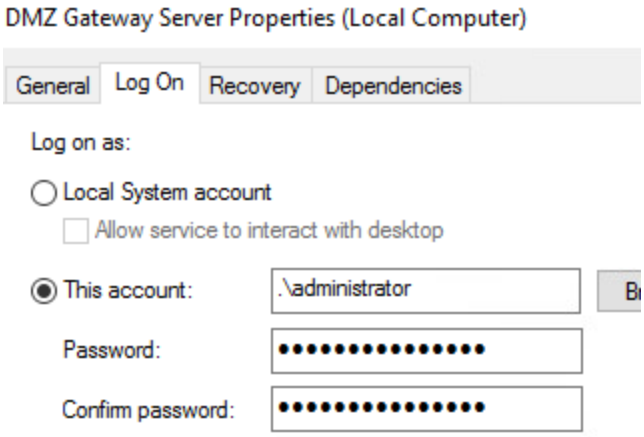
SecurePNCEnabled – This can be set to “true” or “false” to either enable or disable the secure PNC feature. By default this is false. If set to “true” you will also need to at a minimum provide values for the **PNCKeyStorePath**, **PNCStorePassphrase**, **PNCProtocols**, and **PNCCiphers**. If these aren’t set, the **DMZGatewayServer.log**file should contain log entries explaining what is missing.

If the **SecurePNCEnabled** setting is set to true, then it also acts like a “require SSL” setting in that only secure peer notification channels will be allowed. In other words, whether or not a channel is to be secured is enforced by the server and not solely dictated by the client.

PNCKeyStorePath – The full path to a Java keystore file which contains the certificate and private key (pair) that the DMZ Gateway will use for the PNC. By default, this has no value.

PNCKeyStore path supports network locations, however, the DMZ Gateway server service needs to have access to the network share. In this example, the network share on \\192.168.100.143 has the administrator account with access to it.

```
</NetworkAccessPolicy>
<AccelerationIP>AllIPv4</AccelerationIP>
<SecurePNCEnabled>true</SecurePNCEnabled>
<PNCKeyStorePath>\\192.168.100.143\keystore\keystore.jks</PNCKeyStorePath>
<PNCTrustStorePath>\\192.168.100.143\keystore\truststore.jks</PNCTrustStorePath>
<PNCTrustStorePath></PNCTrustStorePath>
<PNCStorePassphrase>OSBEjnEgz80U0x13GeqXroJ2DrQok8173iT19UhlUxGJqSvn508FOd3aVAqJio1EycJqYxy8gD2Ri57b42sa5f2Ytg==</PNCStorePassphrase>
<PNCProtocols>TLSv1.2,TLSv1.1</PNCProtocols>
<PNCCiphers>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECD
```



PNCTrustStorePath [Optional] – The full path to a Java keystore (that is, trust store) file which contains EFT’s certificate (just certificate, not private key) that is specified

on the EFT Site-level **Connections**tab in the **SSL Certificate Settings**dialog box. If a path is provided, client certificate authentication is required, and therefore EFT's certificate must exist in this keystore for the certificate to be trusted. If a path is not provided, then client certificate authentication is not required. By default, this has no value.

PNCStorePassphrase – This is that keystore passphrase for both the keystore and truststore mentioned above. You enter the password verbatim and then when the DMZ Gateway starts it will auto-encrypt the passphrase in the config file. By default, this has no value. PNCStorePassphrase is encoded to protect it from casual observance, but for added security it is recommended that you update the ACLs for the gwconfig.xml file to allow read and write access to only the account under which the DMZ Gateway service runs.

PNCProtocols – A comma separated list of protocols that the DMZ Gateway will allow for the secure PNC. This can take on the following values (by default set to TLSv1.2,TLSv1.1):

- TLSv1.2
- TLSv1.1
- TLSv1
- SSLv3 – This protocol is disabled by default by the JRE. To enable it you must update the java.security file under the install folder of the DMZ Gateway under "bin\jre1.8.0_74\lib\security" and remove SSLv3 from the line below:
- jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA…
- SSLv2Hello

PNCCiphers – Comma-separated list of cipher suites that the DMZ Gateway supports. Defaults to a list of secure ciphers that are supported by OpenJDK v17.0.2.

Per https://docs.oracle.com/javase/7/docs/technotes/guides/security/SunProviders.html#importlimits, Java, by default, limits the encryption strength (that is, maximum key size) for various algorithms due to import regulations in some countries. Therefore, to use stronger encryption like AES 256, you will need to deploy the JCE Unlimited Strength Jurisdiction Policy Files We aren't enabling that by default so that we can make sure we also comply with these import restrictions.

Also, the SSLEngine JCE API doesn't appear to support the cipher suite syntax such as "RSA+AES" or ! so the full cipher suite names must be specified.

Here is an example of the new config settings with sample values:

```
<SecurePNCEnabled>true</SecurePNCEnabled>
 <PNCKeyStorePath>C:\devel\certs\keystore.jks</PNCKeyStorePath>

<PNCTrustStorePath>C:\devel\certs\truststore.jks</PNCTrustStoreP
ath>

<PNCStorePassphrase>GSBEvsavuSo9cA6OO18fS5B+ubI+zdoDBYTzMoA3vtDQ
iiA65hLnVLdRAwyIZStqezbpLnbsu3E1IOH5Fh1Hij9qjQ==</PNCStorePassph
rase>
<PNCProtocols>TLSv1.2,TLSv1.1,TLSv1</PNCProtocols>
<PNCCiphers>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256</PNCCiphers>
```

List of cipher suites

In v4.0 of DMZ Gateway, the JDK/JRE update includes the following updated ciphers in gwconfig.xml:

```
"TLS_AES_128_GCM_SHA256",
"TLS_AES_256_GCM_SHA384",
"TLS_CHACHA20_POLY1305_SHA256",
"TLS_DHE_DSS_WITH_AES_128_CBC_SHA",
"TLS_DHE_DSS_WITH_AES_128_CBC_SHA256",
"TLS_DHE_DSS_WITH_AES_128_GCM_SHA256",
"TLS_DHE_DSS_WITH_AES_256_CBC_SHA",
"TLS_DHE_DSS_WITH_AES_256_CBC_SHA256",
"TLS_DHE_DSS_WITH_AES_256_GCM_SHA384",
"TLS_DHE_RSA_WITH_AES_128_CBC_SHA",
"TLS_DHE_RSA_WITH_AES_128_CBC_SHA256",
"TLS_DHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_DHE_RSA_WITH_AES_256_CBC_SHA",
"TLS_DHE_RSA_WITH_AES_256_CBC_SHA256",
"TLS_DHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA",
"TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
```

```
"TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA",
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
"TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA",
"TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA",
"TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384",
"TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDH_RSA_WITH_AES_128_CBC_SHA",
"TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDH_RSA_WITH_AES_256_CBC_SHA",
"TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384",
"TLS_EMPTY_RENEGOTIATION_INFO_SCSV",
"TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384",
"TLS_RSA_WITH_AES_128_CBC_SHA",
"TLS_RSA_WITH_AES_128_CBC_SHA256",
"TLS_RSA_WITH_AES_128_GCM_SHA256",
"TLS_RSA_WITH_AES_256_CBC_SHA",
"TLS_RSA_WITH_AES_256_CBC_SHA256",
"TLS_RSA_WITH_AES_256_GCM_SHA384"
```

Database Authentication Types

The topics below provide information regarding specifying the user database to use for Site Authentication.

- Authentication Types
- Automatically Updating the User Authentication Database
- Active Directory Authentication
- LDAP Authentication
- ODBC Authentication

Authentication Types

EFT supports the following database types for authenticating users:

- **Globalscape Authentication**(EFT-managed authentication) does not rely on outside sources for user information. All authentication information is:
  - Protected from the operating system
  - Contained within EFT
  - Encrypted and can only be modified through the administration interface
- Active Directory (NTLM/AD) Authentication. Using this method, EFT assigns permissions to users from the NT user database on the system that is running EFT. EFT queries the Primary Domain Controller (PDC) for your domain and adds all domain users to the Settings Template tree.
- LDAP (Lightweight Directory Access Protocol) is a protocol for accessing information directories on an LDAP Server.
- ODBC Authentication allows all users in an external ODBC database to have access to EFT. When upgrading from 7.4.x to 8.0.x, the ODBC schema has changed. If you are using ODBC as the authentication database, then you will need to consult with Globalscape Support so we can assist with the manual process necessary to get EFT updated and running.

Once a Site has been created, you cannot change the authentication method.

Automatically Updating the User Authentication Database

EFT can automatically check the user authentication database at regular intervals to make sure the user information is correct and current. This feature updates EFT only. You can also automatically update the User Authentication Database individually.

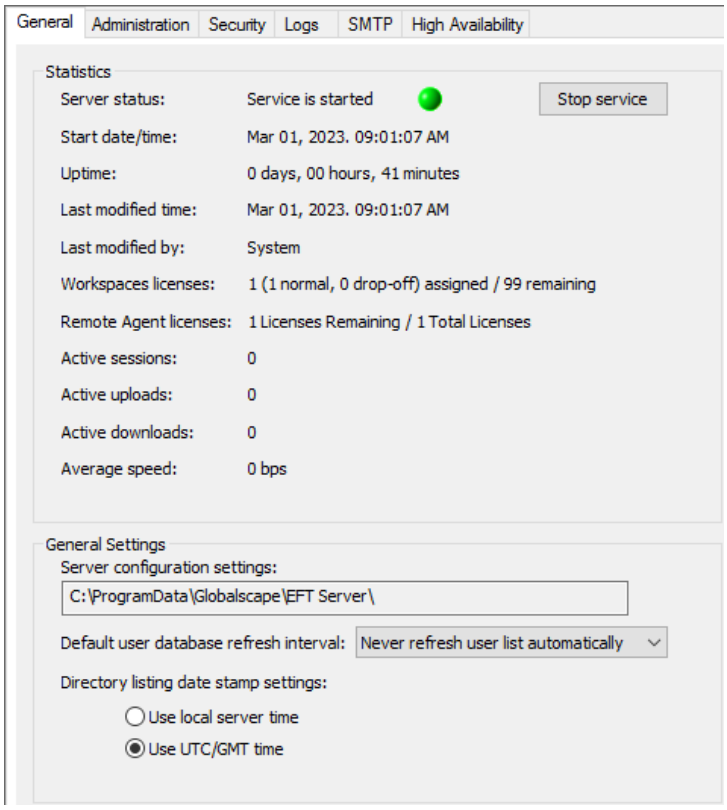
Database refresh should be disabled on EFT nodes used in HA configurations. (Set to **Never refresh user list automatically**.)

Depending on the refresh settings, a user account might not immediately appear in the administration interface when you create the account. When a user account that has not yet appeared in the list attempts to log on, the Server will query the user authentication manager to determine if the user account is authorized to connect to EFT. Once the account has been verified, it will appear in the list.

In the COM API, use `ICISite::ForceSynchronizeUserDatabase`.

To change the update authentication information

1. In the administration interface, click the **Server** tab.
2. On the **Server**tab, click the Server node you want to configure.
3. In the right pane, click the **General**tab.



4. In the **Default user database refresh interval** list, select how often you want the EFT service to check for changes to the authentication database. If you do not want the service to check, click **Never refresh user list automatically**.

Related Topic

- Automatically Updating the User Authentication Database

Active Directory Authentication

The topics below provide information about AD authentication on EFT.

- Local Security Policy Setting when Using Active Directory Authentication
- Support for Foreign Groups (AD Auth)
- Removing Domain from the User Folder Name (AD Auth)
- Changing Windows AD Authentication Options
- Filter Multiple Active Directory Groups

Local Security Policy Setting when Using Active Directory Authentication

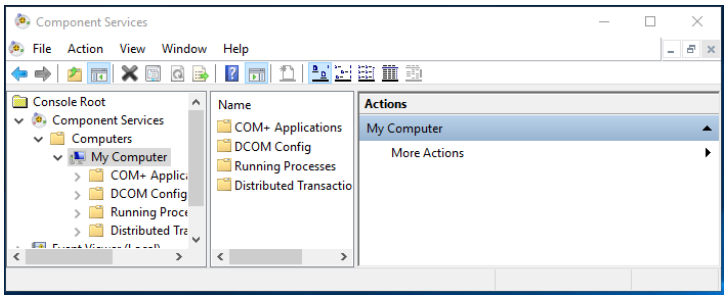
To use AD authentication, Globalscape Customer Support recommends creating an AD account for the EFT service "Log on as" account with adequate privileges to all of the resources (AD domain query, network shares) required for the Site. There is no set formula for the type of account needed, because network configurations vary. Some EFT customers might need to pull users across multiple domains or might want to restrict that kind of access. Consult with your AD network administrator for assistance, if necessary.

If you are using a Domain User account (an AD account that is a member of the Domain Users group and nothing more), make sure that full permissions are granted to the EFT service domain user account in the following locations:

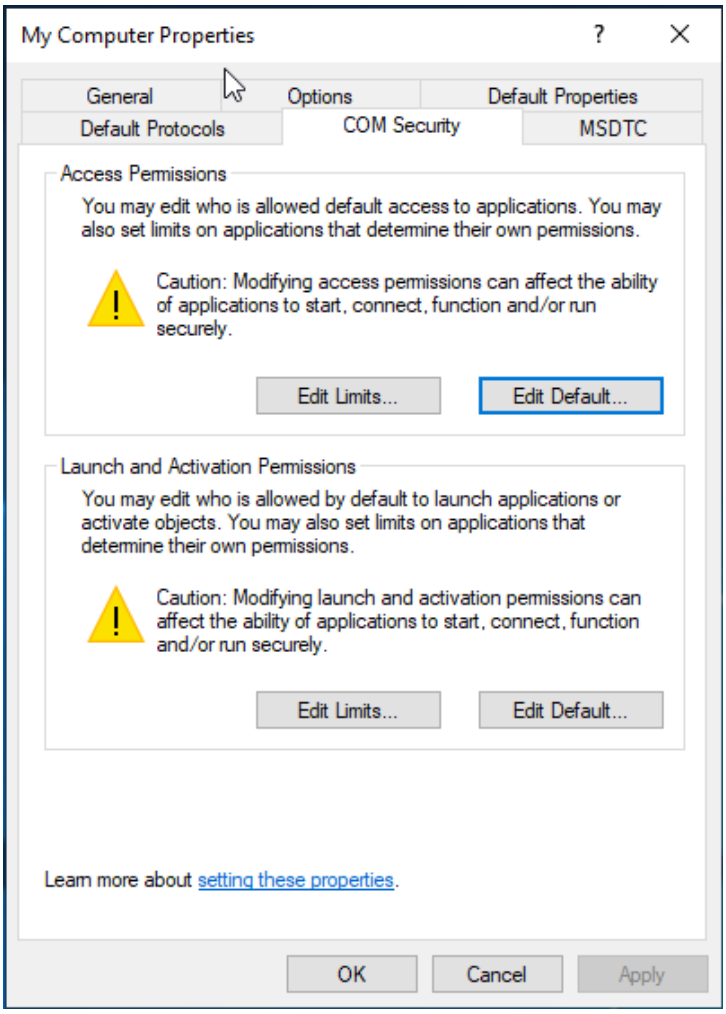
- Installation folder
- Application data folder
- Windows temp folder (varies by system)
- Any shared drive paths required by EFT
- Any output directories to which EFT may need to read/write files

In **Component Services**, provide the appropriate permissions:

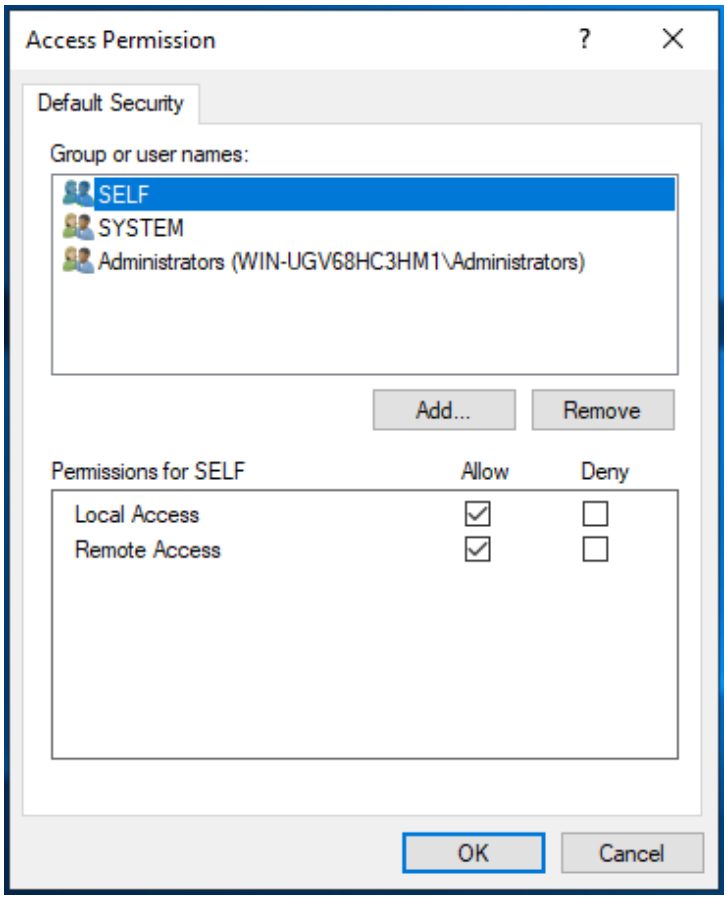
1. Click **Start > Run**, type **dcomcnfg.exe**, then press ENTER. **Component Services** appears.
2. Expand **Component Services > Computers**.



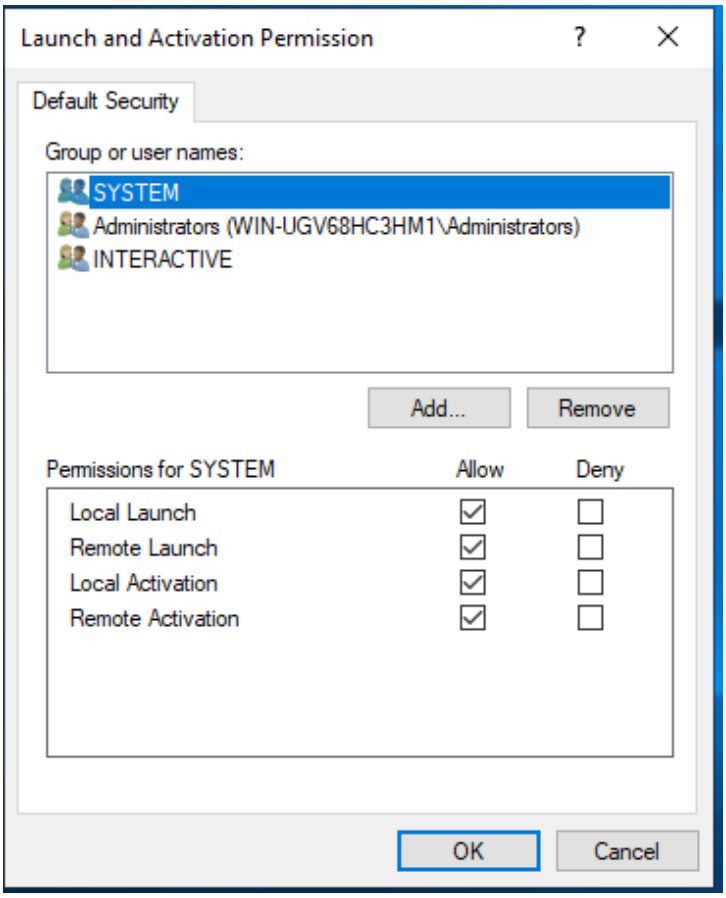
3. Right-click the **My Computer** node, and then click **Properties**. The **My Computer Properties** dialog box appears.



4. Click the **COM Security** tab.
5. Under **Access Permissions**, click **Edit Default**.



6. Add the domain user and then select the **Allow** check box for **Local Access** and **Remote Access**.
7. Click **OK** to close the **Access Permission** dialog box.
8. Under **Launch and Activation Permissions** group, click **Edit Default**.
9. Add the domain user and then select the **Allow** check box for **Local Launch** and **Local Activation**.



10. Click **OK**, then **OK** again, then close **Component Services**.

If you run into issues, run Process Monitor or similar tools and isolate non-success results caused by cftpsai.exe, cftpstes.exe, gsawe.exe, and other EFT processes.

Refer to Support for Foreign Groups for more information.

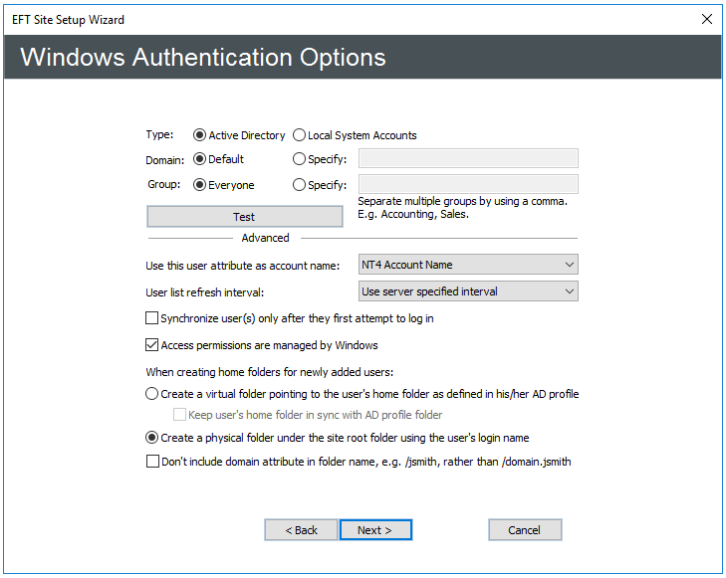
Support for Foreign Groups

EFT allows you to specify only one domain and one group. However, that group can contain groups and users from foreign domains, as long as a trust relationship exists between the domains. This allows users from remote domains to authenticate to EFT. So, as long as a trust relationship exists between the domains, EFT can authenticate users from remote domains. The domain in which EFT resides will need to have a group that contains the foreign domain users.

The main point is that EFT only talks to one AD/forest/controller. If the AD/forest/controller is properly configured to get information from the other domain/forest, then EFT will authenticate those users.

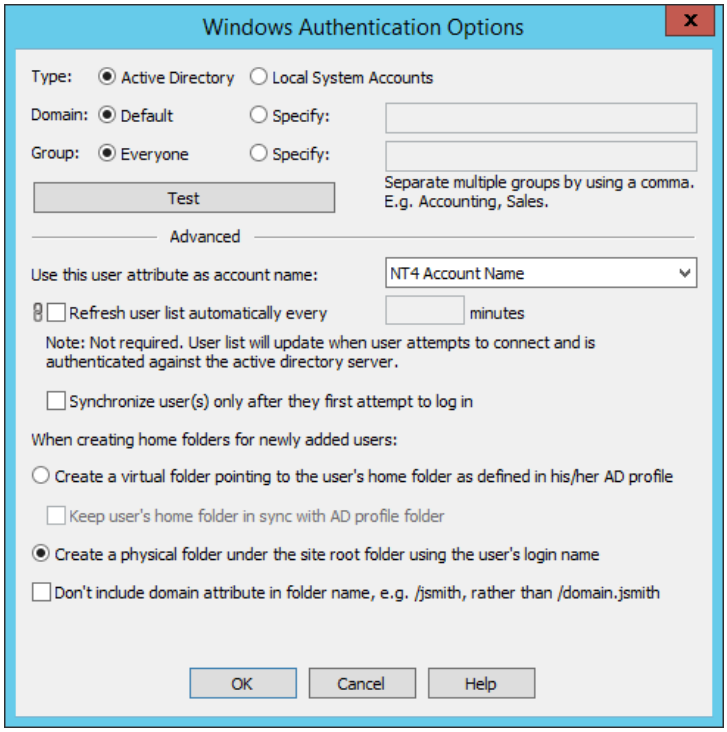
When your forest contains domain trees with many child domains and you observe noticeable user authentication delays between the child domains, you can optimize the user authentication process between the child domains by creating shortcut trusts to mid-level domains in the domain tree hierarchy. For more information, refer to When to create a shortcut trust on Microsoft's website. For details of controlling access to shared resources across domains, refer to the Microsoft TechNet article, Accessing resources across domains.

In the **Windows Authentication** page of the Site Setup wizard, you can specify any combination Domain and Group names, as long as the EFT service is running under an account that has rights to list users in that Domain and/or Group.



Removing Domain from the User Folder Name

The **Use [account] rather than [domain].[account] for folder naming format** check box in the **Windows Authentication Options** configuration (in the Site wizard and on the Site's **General** tab) is selected by default when you are using the **NT4 Account Name** as a logon attribute and if **Create a physical folder under the site root folder** is selected. Without the check box selected, the user's folder in the VFS is named with the domain and the user account (domain.username). Selecting the check box removes the domain from the folder name.



In the examples in the table:

- AD domain name is "win2k3_2.com"
- Domain controller has configuration for user "JDoe"
- Local path: "C:\InetPub\"
- Display Name: "DNJDoe"

Automatically create home folder check box in Site Setup wizard	**Settings Template Home folder (General tab of Settings Template)**	**Logon Name**	**Home folder type**	**Use [account] rather than [domain].[account]**	**Client home folder (Before logging in, no client home folder is defined)**	
					After first login	Actual home folder
Selected ☑	Not Defined	NT4 Account Name	Virtual	Selected ☑	/Usr/JDoe	C:\InetPub
				Cleared ☐	/Usr/WIN2K3_2.1	C:\InetPub
			Physical	Selected ☑	/Usr/JDoe	/Usr/JDoe
				Cleared ☐	/Usr/win2k3_2.1	/Usr/win2k3_2.1
		Display Name	Virtual	**Not available**	/Usr/DisplayNameJDoe	C:\InetPub
			Physical	**Not available**	/Usr/DisplayNameJDoe	/Usr/DisplayNameJDoe
		User Principal Name	Virtual	**Not available**	/Usr/JDoe@win2k3_2.com	C:\InetPub
			Physical	**Not available**	/Usr/JDoe@win2k3_2.com	/Usr/JDoe@win2k3_2.com
		Common Name	Virtual	**Not available**	/Usr/JDoe	C:\InetPub
			Physical	**Not available**	/Usr/JDoe	/Usr/JDoe

Automatically create home folder check box in Site Setup wizard	**Settings Template Home folder (General tab of Settings Template)**	**Logon Name**	**Home folder type**	**Use [account] rather than [domain]. [account]**	**Client home folder (Before logging in, no client home folder is defined)**	
					After first login	Actual home folder
	/Usr/MyUsers	NT4 Account Name	Virtual	Selected ☑	/Usr/MyUsers/JDoe	C:\InetPub
				Cleared ☐	Usr/MyUsers/win2k3_2.1	C:\InetPub
			Physical	Selected ☑	/Usr/MyUsers/JDoe	Usr/MyUsers/JDoe
				Cleared ☐	/Usr/MyUsers/win2k3_2.1	/Usr/MyUsers/win2k3_2.1
		Display Name	Virtual	**Not available**	/Usr/MyUsers/DisplayNameJDoe	C:\InetPub
			Physical	**Not available**	/Usr/MyUsers/DisplayNameJDoe	/Usr/MyUsers/DisplayNameJDoe
		User Principal Name	Virtual	**Not available**	/Usr/MyUsers/JDoe@win2k3_2.com	C:\InetPub
			Physical	**Not available**	/Usr/MyUsers/JDoe@win2k3_2.com	/Usr/MyUsers/JDoe@win2k3_2.com
		Common Name	Virtual	**Not available**	/Usr/MyUsers/JDoe	C:\InetPub
			Physical	**Not available**	/Usr/MyUsers/JDoe	/Usr/MyUsers/JDoe

Automatically create home folder check box in Site Setup wizard	Settings Template Home folder (General tab of Settings Template)	Logon Name	Home folder type	Use [account] rather than [domain].[account]	Client home folder (Before logging in, no client home folder is defined)	
					After first login	Actual home folder
Cleared ☐	Not Defined	NT4 Account Name	**Not available**		Undefined	Site root
		Display Name	**Not available**		Undefined	Site root
		User Principal Name	**Not available**		Undefined	Site root
		Common Name	**Not available**		Undefined	Site root
	/Usr/MyUsers	NT4 Account Name	**Not available**		Undefined	Settings Template folder
		Display Name	**Not available**		Undefined	Settings Template folder
		User Principal Name	**Not available**		Undefined	Settings Template folder
		Common Name	**Not available**		Undefined	Settings Template folder

For details of the Virtual File System (VFS), refer to Virtual File System.

Changing Windows Authentication Options

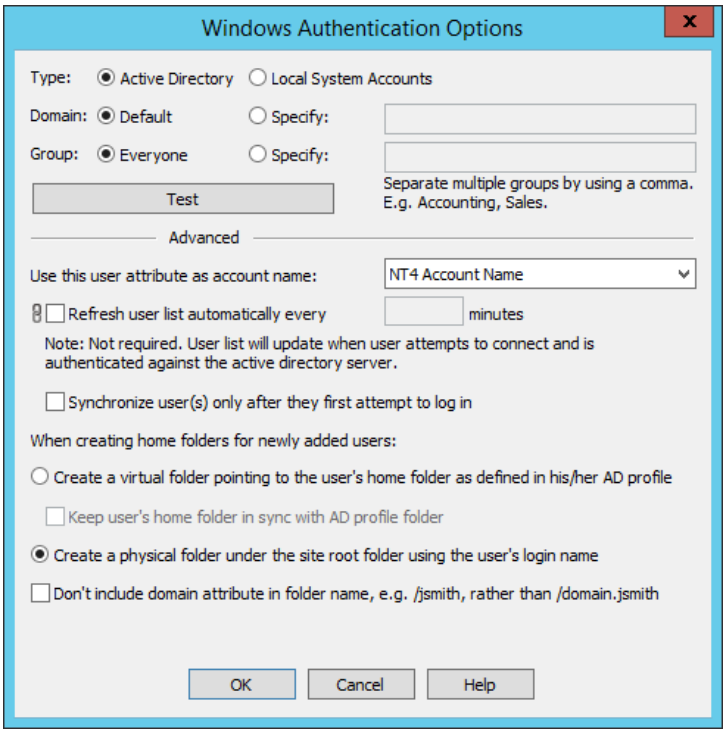
You cannot change the authentication *method*after you have created a Site; however, if you need to change the authentication *options*, you can do so on the **General** tab of the Site. After you change the options, you must manually refresh the administration interface. Any users logged on to the Site will be disconnected if you change the AD configuration and click **OK**, because the Site will stop and then restart. If you remove a logged-on user account from AD, the account is not removed from the interface until after they log off and you refresh the interface.

Regardless of the logon name chosen, EFT will accept the provided logon name type, whether UPN, NT4 account name, common name, or display name, and if a match exists, the user will be authenticated and the chosen logon name type will be displayed in the administration interface.

Logon name type	Allowed login form
NT4 Account Name (NT4)	NT4/UPN
Display Name (DN)	DN/NT4/UPN
User Principal Name (UPN)	UPN/NT4
Common Name (CN)	CN/NT4/UPN

To edit the AD authentication options for a Site

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the AD Site you want to configure.
3. In the right pane, click the **General**tab.
4. Next to the **User auth manager** box, click **Configure**. The **Windows Authentication Options** dialog box appears.



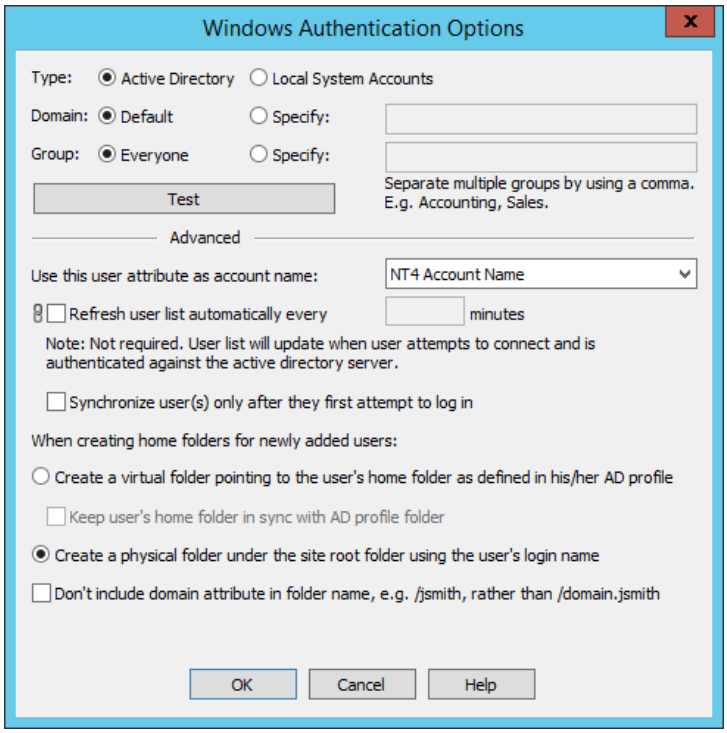
5. To specify that the user list is to be updated automatically, select the **Refresh user list automatically every** check box, then specify how often you want EFT to check the authentication database for new users. Clear the check box if you do not want the Site's user list to refresh automatically.

6. When you created the Site, you specified either **Active Directory** or **Local System Accounts**. If you need to change this, click the appropriate option to match the authentication method used on EFT's domain. Authentication is done with the `LogonUser()` function. The operating system determines which method to use for authentication, such as Kerberos, NTLM2, etc.
    - **Active Directory** - EFT queries the domain controller for a list of users and groups.
    - **NTLM Authentication**- EFT queries the local system to get the list of users and groups.
7. In the **Domain**area, do one of the following:
    - Click **Default**if you want to use the authentication database from the computer's current domain.
    - Click **Specify**, then in the box, provide the domain name that contains the authentication database.
8. In the **Group**area, do one of the following:
    - To allow access to every user in the domain's database, click **Everyone**.
    - To allow access to only a specific AD Group, click **Specify**, then in the box, type the AD Group name for users that will have access to the Server.
9. In the **Use this user attribute as the logon name** box, click the list to specify the attribute to use (only available when AD authentication is selected):
    - **NT 4 Account Name** - Domain name (for example, "globalscape\bsmith" or "bsmith")
    - **Display Name** - (DN) When a new user is created in Active Directory, the Full name field is always generated in FirstName LastName format (but can be changed manually). This field sets the Display Name field upon account creation.
    - **User Principal Name** - (UPN) Login name in email format. For example, your_user_name@mycompany.com
    - **Common Name** - (CN) Dynamic name. Usually the same as Display Name. However if Display Name is blank, then it will be NT4 account name.
10. In the **When creating home folders for newly added users** area, specify whether you want the Site to **Create a virtual folder pointing to the user's home folder as defined by AD**or **Create a physical folder under the site root folder using the user's login name**.
    (These options are not available if the **Automatically create home folder for new users** check box is cleared on the **Security** tab of the Site. This setting affects all users on this Site, including existing user accounts.)

11. The **Use [account] rather than [domain].[account] for folder naming format** check box is selected by default when you are using the **NT4 Account Name** as a logon attribute and if **Create a physical folder under the site root folder** is selected. Without the check box selected, the user's folder in the VFS is named with the domain and the user account (domain.username). Selecting the check box removes the domain from the folder name. Refer to Removing Domain from the User Folder Name for more information.
12. To verify your settings, click **Test**. The **Authentication Manager Test Results** dialog box appears and EFT attempts to connect to the domain controller to get the user list. If it is successful, the list of registered users appears in the tree under the Settings Template. To close the dialog box, click **Close** or press ESC.
13. Click **OK** to save the settings. Any users who were logged in to the Site will be disconnected, because the Site will stop and then restart.
14. Click **Apply**to save the changes on EFT.

Filter Multiple Active Directory Groups

You can filter for multiple Active Directory groups. For example, if users exist in both Technical and Marketing, you would add those two groups in the **Group** field, separated by a comma.



Related Topics

- Creating a Site
- Changing Windows AD Authentication Options

LDAP Authentication

The topics below provide information about LDAP authentication on EFT. See Creating a Site for information about creating an LDAP-authenticated Site.

- Understanding LDAP Authentication
- Advanced LDAP Filtering
- Map LDAP Account Attributes to EFT User Account Details
- Allow LDAP Authentication through DMZ
- Specifying External and Internal Domains
- Connecting to an LDAP Server
- Map LDAP Users to a Settings Template
- Changing and Testing LDAP Authentication Options
- User Home Folders on an LDAP-Authenticated Site
- Removing Inactive LDAP Accounts from EFT
- Using Sun Directory LDAP Server
- Configuring CAC on an Existing LDAP Site
- Common Access Card (CAC) Authentication

Understanding LDAP Authentication

EFT supports using an LDAP (Lightweight Directory Access Protocol) directory service for authenticating users. A typical LDAP directory service is a simple network-accessible database in which user account lists are stored and includes information about those users and the privileges assigned to each user. LDAP support on EFT allows you to authenticate users through connection to LDAP servers such as Novell eDirectory server, OpenLDAP, Sun ONE Server, Microsoft's Active Directory server, and Tivoli Access Manager.

This help file is not intended as an LDAP tutorial. For information about LDAP, refer to LDAP in the Microsoft MSDN Library.

Related Topics

- Connecting to an LDAP Server
- LDAP Filtering
- Testing LDAP Authentication Settings
- Defining Connections (Sites)
- Allow LDAP Authentication through DMZ

Advanced LDAP Filtering

EFT's LDAP authentication manager allows you to create complex filters for retrieving sub-sets of users across your LDAP directory, similar to retrieving users only in a specific group in Active Directory. The Server follows the filtering conventions outlined in http://www.faqs.org/rfcs/rfc2254.html.

User updates is an asynchronous process; therefore, other administration interface updates may be ongoing, causing a delay in the presentation of the user updates.

LDAP filtering is a complex task that requires an advanced understanding of LDAP. For detailed information, please refer to RFC 2252 - Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions, RFC 2251 - Lightweight Directory Access Protocol (v3), and RFC 2254 - The String Representation of LDAP Search Filters. The operators used in the search filter (&, |, =, ~=, etc.) are defined in RFC 2254.

When you ***How EFT Sites are Defined* on page 596**, you must specify the **User Filter** on the **LDAP Authentications**page of the wizard. You can also specify or edit the user filter in the LDAP Authentication Options dialog box.

The default **User Filter** is `(objectClass=person)`. This means that every ObjectClass attribute of a particular entry of type `person` will be returned in the search result, which may be highly inefficient if you want to authenticate only the users in your marketing department.

Each entry in an LDAP tree consists of one or more attributes that define that entry. Each attribute has a name (attribute type) and is assigned one or more values. The entry itself is defined using a unique identifier, such as its Distinguished Name (dn), that is constructed from selected attributes in the entry followed by the parent's dn, such as: `cn=john smith,dc=example,dc=com`.

Below is a sample entry, with its attributes and values:

```
dn: cn=Jane Smith,dc=example,dc=com

cn: Jane Smith

givenName: Jane

sn: Smith

telephoneNumber: 555 1234

telephoneNumber: 555 5678

mail: jsmith@example.com
```

```
manager: cn=Alma Mia,dc=example,dc=com

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: person

objectClass: top
```

The **User Filter** field appends a filter to the LDAP search query so that only the entries that match the filter are retrieved. A default filter is provided that verifies the ObjectClass attribute of a particular entry is of type `person`. There can be many other types, such as `printer`.

Suppose you only want to pull users from an Organization Unit (ou) container (similar to a group under AD) that is a couple of levels removed from the root Organization (o) container. In this case, simply applying a filter where `(objectClass=person)` pulls users from the entire organization, instead of just the desired OU. Pulling users from the desired OU is accomplished by defining a more complex filter, as described below.

Below is an example of an LDAP directory with multiple ou under an o:

```
[-] o=Globalscape

[-] ou=ResearchAndDevelopment

cn=jbond

cn=jsmith

[-] ou=HumanResources

cn=jdoe

[+] ou=Marketing

[+] ou=PM
```

Below are the entry properties for ResearchAndDevelopment and for one of the entries contained within that ou.

For ResearchAndDevelopment:

```
DN: ou=ResearchAndDevelopment,o=MyOrganization
```

```
ObjectClass: Top

ObjectClass: OrganizationalUnit

ObjectClass: ndsLoginProperties

ObjectClass: ndsContainerLoginProperties

Ou: ResearchAndDevelopment
```

And for jbond:

```
DN: cn=jbond,ou=ResearchAndDevelopment,o=MyOrganization

ObjectClass: Person

ObjectClass: ndsLoginProperties

ObjectClass: Top

GroupMembership: cn=TestGroup,o=MyOrganization

sn: bond

cn: jbond
```

Suppose you want to pull all users of ObjectType = Person from the R&D and HR ous, but not any users from Marketing and PM. The filter would be:

```
(&(objectClass=person)(|(ou:dn:=ResearchAndDevelopment)
(ou:dn:=HumanResources)))
```

The filter above is called an *extensible match search* because it specifies an attribute name: `ou`and the DN's attributes should be considered as part of the entry.

If you had used `ou:=`rather than `ou:dn:=`, no results would have been returned, because the `ResearchAndDevelopment`entry does not match the `objectClass=person`criteria and `jbond`(which does have an `objectClass=person`) does not match the `ou=ResearchAndDevelopment`criteria EXCEPT for the fact that it does have `ou=ResearchAndDevelopment`as part of that entry's Distinguished Name (dn). Therefore `ou:dn:=ResearchAndDevelopment` DOES return jbond as one of the users in the search result.

Below is a similar query, except that Mr. Bond is excluded using an exclusion filter and including everyone else under R&D and HR.

```
(&(&(!(cn:dn:=jbond))(|(ou:dn:=ResearchAndDevelopment)
(ou:dn:=HumanResources)))(objectclass=Person))
```

Here is an example of pulling all users from all ou except those in the R&D and HR containers:

```
(&(!(|(ou:dn:=ResearchAndDevelopment)(ou:dn:=HumanResources)))
(objectClass=person))
```

The filter above includes all entries that have an ObjectClass attribute equal to person, but do not return any entries where ResearchAndDevelopment or HumanResources is specified as an ou attribute in the dn.

Here is one last example that retrieves a user with an `objectClass=person`attribute and a `groupMembership`attribute equal to `cn=TestGroup,o=MyOrganization.`

```
(&(objectclass=Person)(groupMembership=cn=TestGroup,o=
 MyOrganization))
```

The use of `value=value=value`in the above example can be confusing. In this case the entire string that follows the first equal sign after `groupMembership`must match `cn=TestGroup,o=MyOrganization`, which is the case for the jbond entry.

Once you have defined a filter, click **Test**to verify the results, before continuing with ***How EFT Sites are Defined* on page 596** or editing the LDAP authentication options.

More examples:

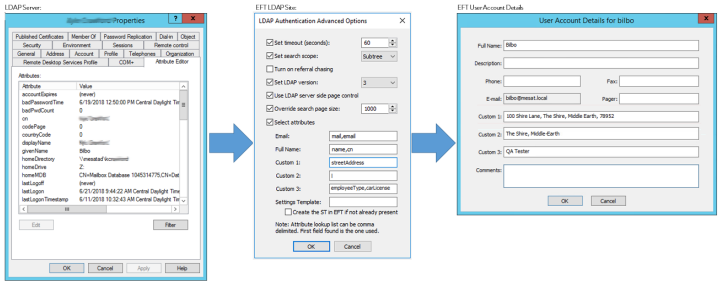
Search filter	Description
(objectClass=*)	All objects
(&(objectCategory=person)(objectClass=user)(!cn=andy))	All user objects but "andy"
(sn=sm*)	All objects with a surname that starts with "sm"
(&(objectCategory=person)(objectClass=contact)(|(sn=Smith)(sn=Johnson)))	All contacts with a surname equal to "Smith" or "Johnson"

Map LDAP Account Attributes to EFT User Account Details

EFT makes it easy to map LDAP attributes to the associated account on an LDAP Site in EFT.

In EFT, the account-specific details associated with a particular user, such as phone number, pager, and email address, are configured on the **Details** tab of a selected user account. Some of these fields (such as the email address) can be used in other areas (such as the Event Rules) to notify the user of a completed transaction. Three Custom fields and Comments field are available for additional details.

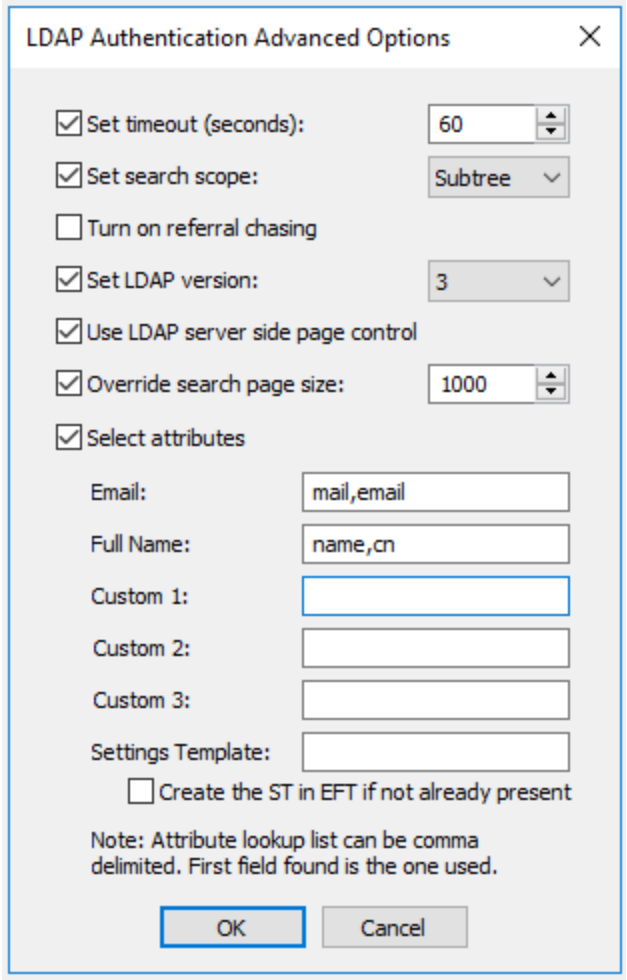
EFT provides the **LDAP Authentication Advanced Options** dialog box in which you can specify the attributes from the LDAP server to populate the **User Account Details**.



To map LDAP attributes to EFT user accounts

1. Do one of the following:
    - On the LDAP Site's **General** tab, click **Configure**, then click **Advanced**.
    - If you are creating a new LDAP site, on the **LDAP Authentication** page of the Site Setup wizard, click **Advanced**. The **LDAP Authentication**

Advanced Options dialog box appears.



2. Select the **Select attributes** check box, then specify the LDAP attributes that you want to use, such as cn (common name), streetAddress, mail (email address), employeeID, employeeType, etc.
    - Multiple attributes can be added to each **Custom** field, but only the first attribute found will be used; All other attributes will be ignored.
    - An attribute field on the LDAP server can contain multiple attributes if you want multiple attributes added to a single **Custom** field, such as for the address.

Allow AD/LDAP Authentication to EFT through DMZ Gateway

Suppose an EFT administrator wants to create an environment in which users in their internal network (as specified by their AD/LDAP server) can access the server to do whatever they want; however, they do NOT want those employees to visit the server from outside their own offices. They also have Workspaces participants that are outside the company, and they need to distinguish INTERNAL access from EXTERNAL access.

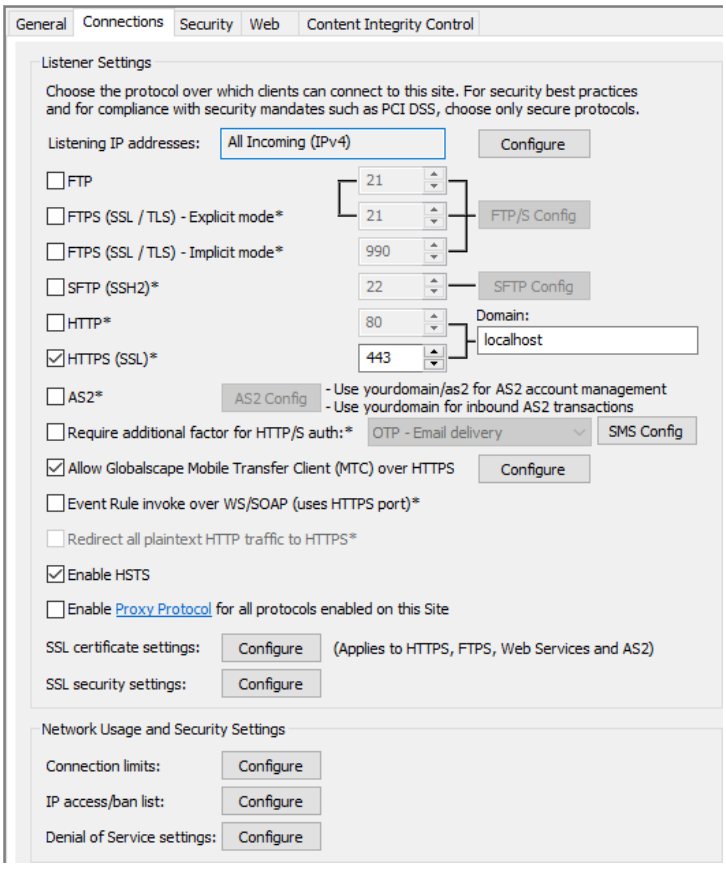
Described below is a way to set a host name for their DMZ Gateway (internet facing) entry to EFT, and anything flowing into EFT from that path will be considered EXTERNAL. Allowing LDAP authentication to EFT through DMZ Gateway is only for directly signing into WTC (not clicking Workspace in a notification email).

(See also Specifying External and Internal Domains and Internal Domain Settings dialog box in Site configuration.)

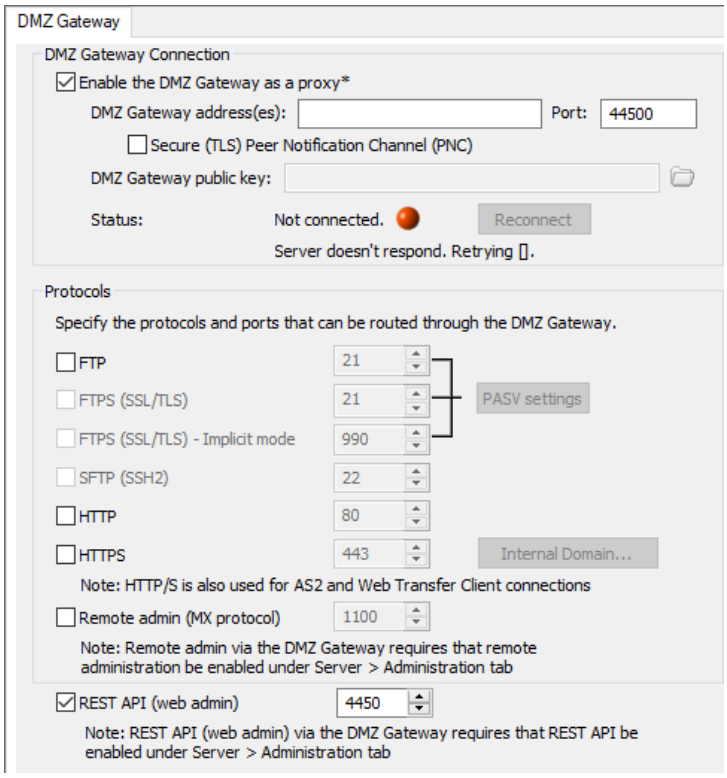
Hyperlinks in Workspaces notification emails are composed **based upon recipient domain**:

- External Users will be directed towards the domain address on the site-connections tab
- Internal Users will be directed towards the address on the internal domain button of the DMZ Gateway

The *external domain* is specified on the Site's **Connections**tab:


General
Connections
Security
Web
Content Integrity Control
Listener Settings
Choose the protocol over which clients can connect to this site. For security best practices and for compliance with security mandates such as PCI DSS, choose only secure protocols.
Listening IP addresses:
All Incoming (IPv4)
Configure
FTP
21
FTPS (SSL / TLS) - Explicit mode*
21
FTPS (SSL / TLS) - Implicit mode*
990
FTP/S Config
SFTP (SSH2)*
22
SFTP Config
HTTP*
80
HTTPS (SSL)*
443
Domain:
localhost
AS2*
AS2 Config
- Use yourdomain/as2 for AS2 account management
- Use yourdomain for inbound AS2 transactions
Require additional factor for HTTP/S auth:*
OTP - Email delivery
SMS Config
Allow Globalscape Mobile Transfer Client (MTC) over HTTPS
Configure
Event Rule invoke over WS/SOAP (uses HTTPS port)*
Redirect all plaintext HTTP traffic to HTTPS*
Enable HSTS
Enable Proxy Protocol for all protocols enabled on this Site
SSL certificate settings:
Configure
(Applies to HTTPS, FTPS, Web Services and AS2)
SSL security settings:
Configure
Network Usage and Security Settings
Connection limits:
Configure
IP access/ban list:
Configure
Denial of Service settings:
Configure

An **Internal Domain** is specified on the **DMZ Gateway** tab:

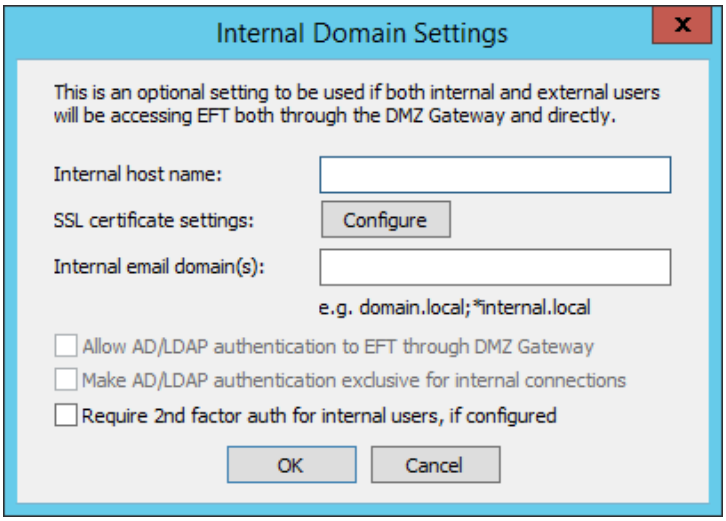


Hyperlinks in notification emails are composed based upon recipient domain

- In the **DMZ Gateway**tab **Internal Domain** settings, the internal email domain list, similar to email domain list in Workspaces Drop-Off tab, is, by default, empty. Empty means no email domain matching is performed and links are not altered.
- In the **DMZ Gateway**tab **Internal Domain** settings, the internal host name is, by default empty. Empty means that no domain matching is performed and links are not altered.
- If EFT sends an email where the email domain (after the "@" symbol) matches one of the specified "internal domains" values, any URLs formed by EFT and pointing to EFT in the email should be constructed using the internal host name (for example, mft2go.internal.com).
- If no internal host name was specified, then EFT will use the default host name.
- If EFT sends an email where the email domain (after the "@" symbol) matches NONE of the specified "internal domains" values, any URLs formed by EFT and pointing to EFT in the email should be constructed using the default host name specified in the DMZ Gateway tab.

To specify the internal domain on an LDAP site

1. In the EFT administration interface, click the **Server**tab, then click the **Gateway** node.
2. On the **DMZ Gateway** tab, next to the **HTTPS**port box, click **Internal Domain**. The **Internal Domain Settings**dialog box appears.

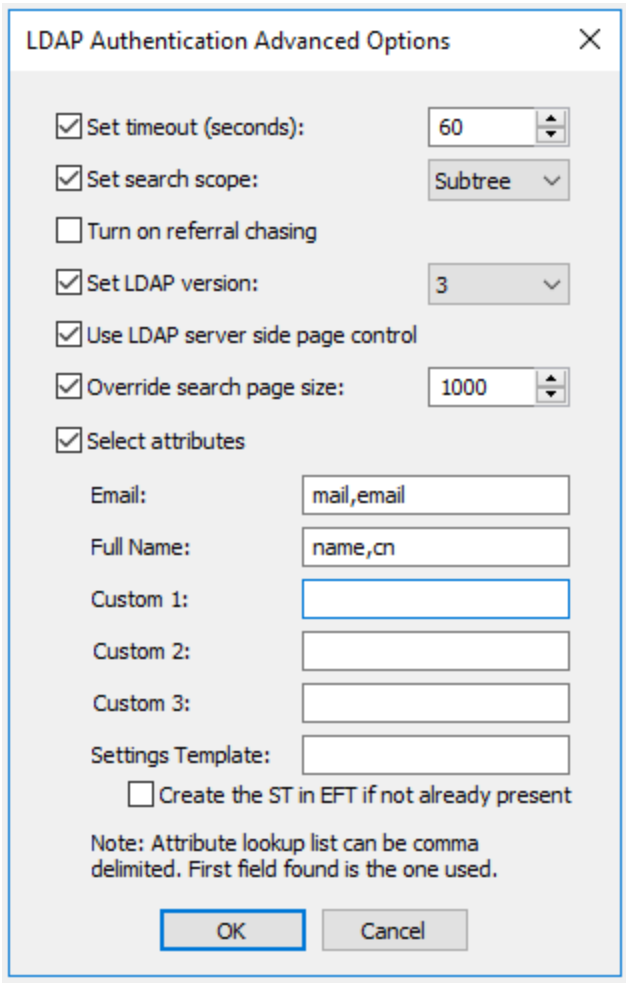


> **NOTE:** Only invitation emails sent to these domains will include this alternate link address. All others will point to the default links.

3. In the **Internal host name** box, specify the URL through which internal users should log in to EFT.
4. Click **Configure**to specify the SSL certificate settings.
5. In the **Internal email domain(s)** box, specify one or more SMTP domains used by internal users, separated by semicolons.
6. (optional) To allow internal AD or LDAP accounts to authenticate to EFT through DMZ Gateway, select the **Allow AD/LDAP authentication to EFT through DMZ Gateway** check box. (Cleared by default.)
7. (optional) To allow AD or LDAP authentication available only for internal accounts, select the **Make AD/LDAP authentication exclusive for internal connections** check box. (Cleared by default.)
8. (optional) To enable two-factor authentication for internal domain users, select the **Require 2nd factor auth for internal users** check box. (Cleared by default.)
9. Click **OK**.

To specify a custom LDAP attribute to populate user's email at Site and Settings Template level

1. On the LDAP Site's **General** tab, click **Configure**. The **LDAP Authentication Options** dialog box appears.
2. Click **Advanced**. The **LDAP Authentication Advanced Options** dialog box appears.



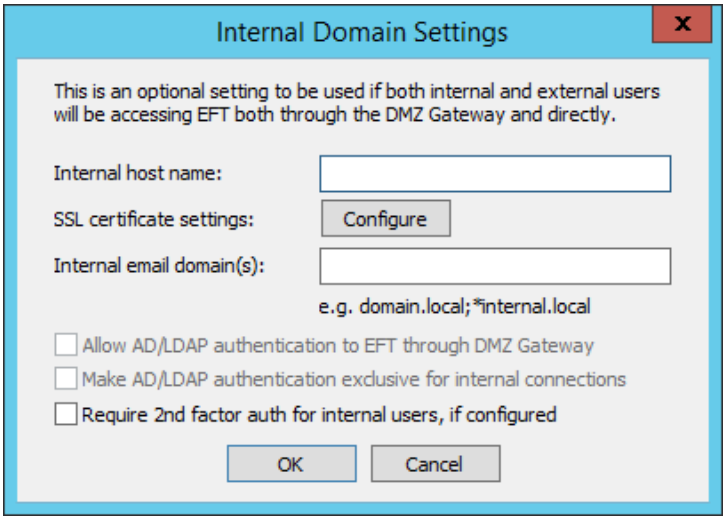
Custom Attributes:

- Multiple attributes can be added to each custom field, but only the first attribute will be used; All other attributes will be ignored
- An attribute field on the AD/LDAP server can contain multiple attributes if you want multiple attributes added to a single custom field (example: address)

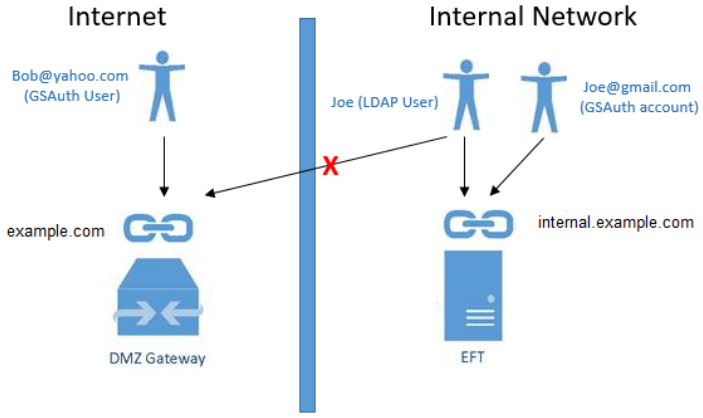
If a user account has been removed from EFT due to inactivity, the user can still log in to Workspaces. The account will be added back to EFT after they log in.

Internal Domain Settings

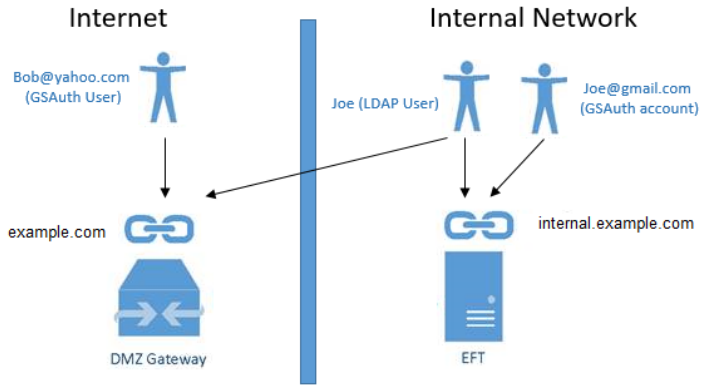
The **Internal Domain Settings**dialog box on the **DMZ Gateway**tab, is used to configure separate external and internal domain access. See Specifying External and Internal Domains and Allow LDAP Authentication through DMZ for more information about how to do that. Below are some diagrams to visually describe how the two check boxes, **Allow AD/LDAP authentication to EFT through DMZ Gateway** and **Make AD/LDAP authentication exclusive for internal connections**, interact to determine external and internal user access.



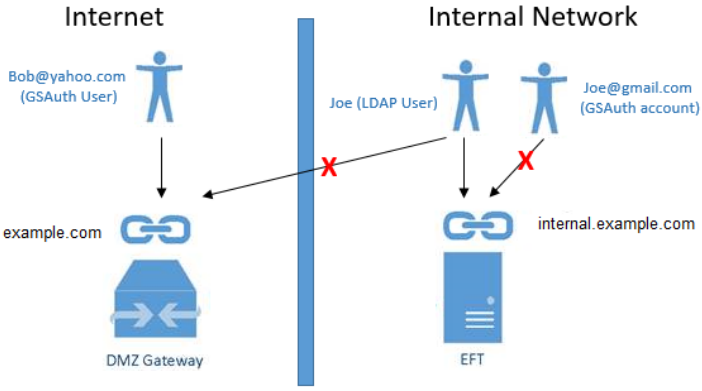
1. When neither box is selected, EFT and DMZ Gateway are in a "split domain" configuration:
    - AD and LDAP users are only allowed to log in through the internal (EFT) URL; they cannot use the external (DMZ Gateway) URL.
    - Globalscape authentication users can log in through the external (DMZ Gateway) URL or the internal (EFT) URL.



2. When the **Allow AD/LDAP authentication to EFT through DMZ Gateway** check box is selected, (but ***not*** the **Make AD/LDAP authentication exclusive for internal connections** check box):
    - Globalscape authentication users and LDAP users can log in using the internal (EFT) URL OR external (DMZ Gateway) URL. This configuration allows remote users to access EFT through DMZ Gateway.

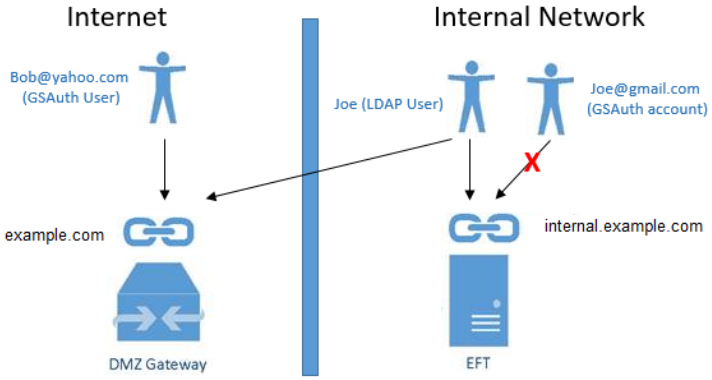


3. When the **Make AD/LDAP authentication exclusive for internal connections** check box is selected (but ***not*** the **Allow AD/LDAP authentication to EFT through DMZ Gateway** check box):
    - LDAP users can only log in using the internal (EFT) URL; they cannot use the external (DMZ Gateway) URL
    - Globalscape authentication users can log in using only the external (DMZ Gateway) URL; they cannot use the internal (EFT) URL



4. When both the **Allow AD/LDAP authentication to EFT through DMZ Gateway** check box and the **Make AD/LDAP authentication exclusive for internal connections** check box are selected:

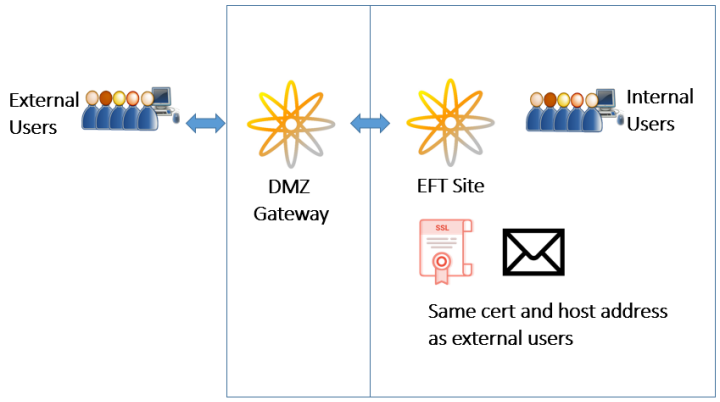
- Only AD or LDAP users can log in using the internal (EFT) or external (DMZ Gateway) URL
- Globalscape authentication users can only log in using the external (DMZ Gateway) URL; they cannot log in using the internal (EFT) URL.



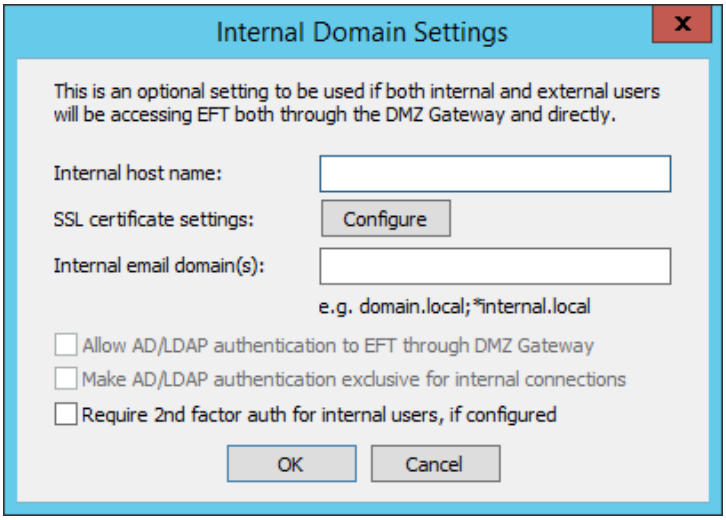
Specifying External and Internal Domains

(See also Allow LDAP Authentication through DMZ Gateway and Internal Domain Settings dialog box.)

By default, an EFT Site uses the same host address and SSL certificate, and email notifications create links to the same host address, as shown below.



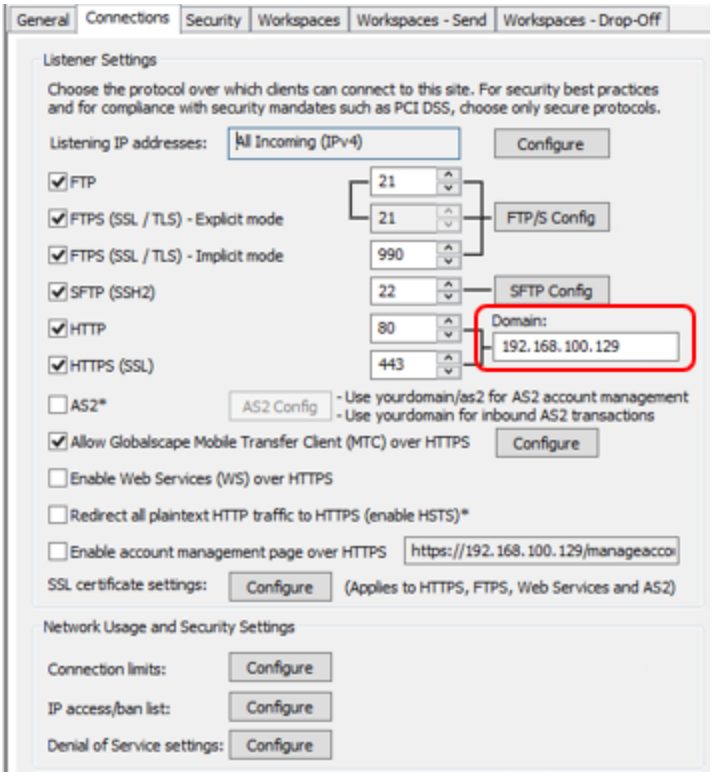
But suppose you want to create an environment in which users in their internal network can access EFT while at their internal workstation, but, for security reasons, you don't want those employees to connect to the server from outside the offices, such as when they are working at the local coffee shop or at a partner location. Also suppose that your company wants to segregate Workspaces participants that are external to the company network, such as vendors and customers.



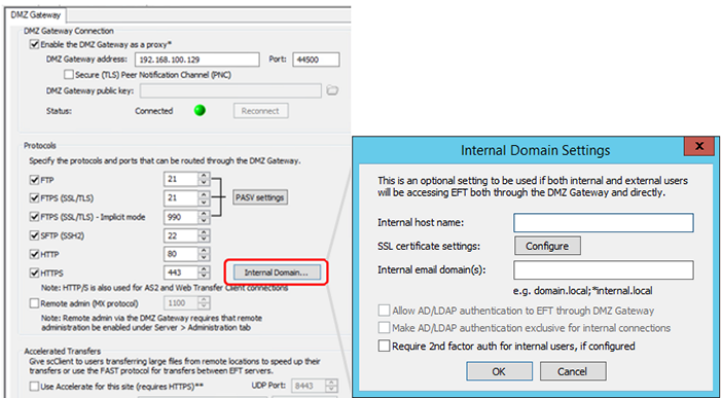
If you want EFT to distinguish INTERNAL access from EXTERNAL access, you can specify a host address for DMZ Gateway (Internet-facing) entry to EFT, and anything

flowing into EFT from that path will be considered external, then specify a different host address for internal users, as described below.

The *external domain* is specified on the Site's **Connections** tab:



An **Internal Domain** button is available next to the **HTTPS** port box on the **DMZ Gateway** tab of the EFT Site:



To specify the internal domain on a site

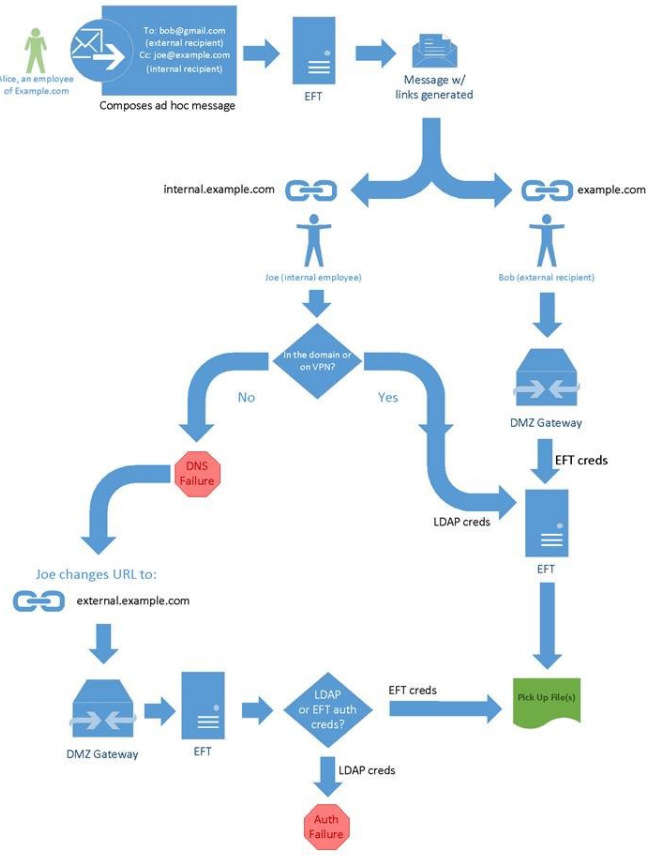
1. In the EFT administration interface, click the **Server**tab, then click the **Gateway** node.

2. On the **DMZ Gateway** tab, next to the **HTTPS** port box, click **Internal Domain**. The **Internal Domain Settings** dialog box appears.
3. In the **Internal host name**box, specify the URL through which internal users should log in to EFT. **Internal host name** is empty by default. Empty means that no domain matching is performed and notification links are not altered.
4. Click **Configure** to specify the SSL certificate. Internal users can use a different SSL certification than the external users. For example, for internal connections, and self-signed certificate created by EFT should be adequate.
5. In the **Internal email domains**box, specify one or more SMTP domains used by internal users, separated by semicolons. **Internal email domain**is empty by default. Empty means no email domain matching is performed and notification links are not altered.
6. Select the check boxes as needed:
    - **Allow LDAP authentication to EFT through DMZ Gateway** - Allows anyone connecting to EFT through DMZ Gateway to connect using LDAP authentication
    - **Make LDAP authentication exclusive for internal connections** - Prevents external connections to EFT through DMZ Gateway over LDAP
    - **Require 2nd factor auth for internal users** - Requires internal connections to EFT through DMZ Gateway to connect using LDAP authentication to use two-factor authentication, such as RSA SecurID
7. Click **OK**.

Workspaces Invitation and Notification Email Links

With separate internal and external domains defined, you can send different notification emails to internal and external accounts from the same EFT Site:

- If EFT sends an email where the email domain (after the "@" symbol) matches one of the specified "internal domains" values, any URLs formed by EFT and pointing to EFT in the email should be constructed using the internal host name (for example, internal.example.com).
- If EFT sends an email where the email domain (after the "@" symbol) does not match any of the specified "internal domains" values, any URLs formed by EFT and pointing to EFT in the email should be constructed using the default host name specified in the DMZ Gateway tab (for example, example.com).
- If no internal host name was specified, then EFT will use the default host name.

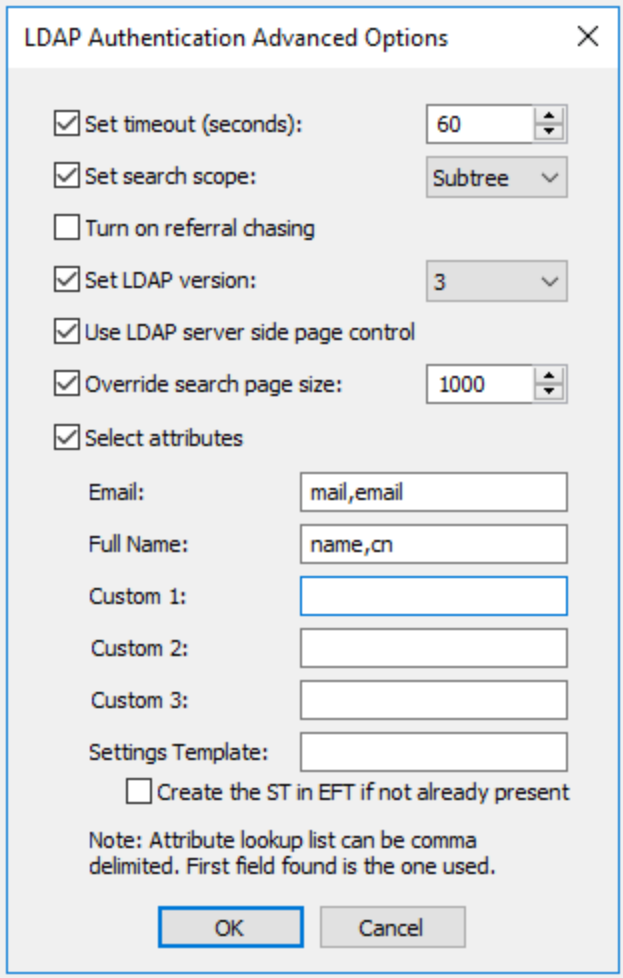

Alice, an employee of Example.com
To: bob@gmail.com (external recipient)
Cc: joe@example.com (internal recipient)
Composes ad hoc message
EFT
Message w/ links generated
internal.example.com
example.com
Joe (internal employee)
Bob (external recipient)
In the domain or on VPN?
No
Yes
DMZ Gateway
EFT creds
DNS Failure
LDAP creds
EFT
Joe changes URL to:
external.example.com
DMZ Gateway
EFT
LDAP or EFT auth creds?
EFT creds
Pick Up File(s)
LDAP creds
Auth Failure

Map LDAP Users to a Settings Template

When a user is added to EFT via connection to the LDAP directory service, they can be automatically added to an LDAP-specific Settings Template rather than the Default template.

To specify the Settings Template for LDAP users

- In the LDAP Authentication Advanced Options dialog box, provide the Settings Template name or select the **Create the ST in EFT if not already present** check box, then click **OK**.



(Refer to Changing and Testing LDAP Authentication Options or Creating a Site for instructions for accessing and configuring this dialog box.)

The user account logon name appears in the Title bar of the **User Account Details** dialog box. Even when the EFT administrator does not have **Manage Personal Data**

enabled, the logon name for the user account will appear in the Title bar, Settings Template tree, and in logs. For additional user privacy, the EFT administrator and users can specify safer login attributes. For example, by default, an LDAP Site uses the "cn" attribute for the account name. Instead, when creating an LDAP Site, the administrator can use "sAMAccountName" as the login attribute, to avoid compromising client full names.

Connecting to an LDAP Server

You can create an LDAP-authenticated Site and connect to an LDAP server. To enable LDAP SSL, you need to have a certificate that includes server authentication on the LDAP server you are connecting to. If you install Certificate Services on the domain on which you install EFT, you can request the certificate on the LDAP server. For more information, refer to the Microsoft Support article "How to enable LDAP over SSL with a third-party certification authority."

When you create a Site that uses LDAP authentication, you will need to provide the following information:

- **IP address/Domain Name** of the LDAP server
- **Port** of the LDAP server. The default is port 389; port 636 for SSL connections.
- **Base DN** base distinguished name that specifies the necessary domain components of the LDAP server. Some LDAP systems, such as Sun ONE Server and Microsoft's Active Directory server, require the organizational unit ("ou") that houses the users on that LDAP server to be included in the BaseDN to allow users to authenticate successfully. The organizational unit is the parent object that contains the user objects. EFT allows you to browse a list of LDAP base DNs from the LDAP server on the domain specified or the default domain. Click **List DNs** to select from the list or type it in the **Base DN** box.

  For example, if the classObject that holds user accounts is **person**, the hierarchical parent node/container could be the organizational unit **people**. If the organizational unit is required by your LDAP server, prepend it to the distinguished name. For example:

  - With Organizational Unit:

    ```
    ou=people,dc=forest,dc=tree,dc=branch
    ```

  - Without Organizational Unit:

    ```
    dc=forest,dc=tree,dc=branch
    ```

- **User Filter**that EFT uses to query the LDAP server for a list of users. The default setting is:

  ```
  objectClass=person
  ```

This finds the LDAP entries that are part of the objectClass person; that is, it retrieves the users on the LDAP server that belong to the person `ObjectClass`.

- **Attribute**that denotes user names in the LDAP database. This allows you to specify the attribute from the queried list of users that denotes user names. Commonly used attributes are **cn**or **uid**.

- **User Information**defines how the client is authenticated. When you configure an LDAP Site, you are asked to choose one of the following binding methods:
  - **Anonymous**
  - **Simple**requires a username and password. Note that the username must follow the syntax for the LDAP server that includes the Common Name and the Domain Components of your LDAP server's distinguished name. For example, the username might be the following:

    ```
    cn=Manager,dc=forest,dc=tree,dc=branch
    ```

- **Advanced Options**- You can specify SSL encryption and the frequency with which the user list is refreshed.

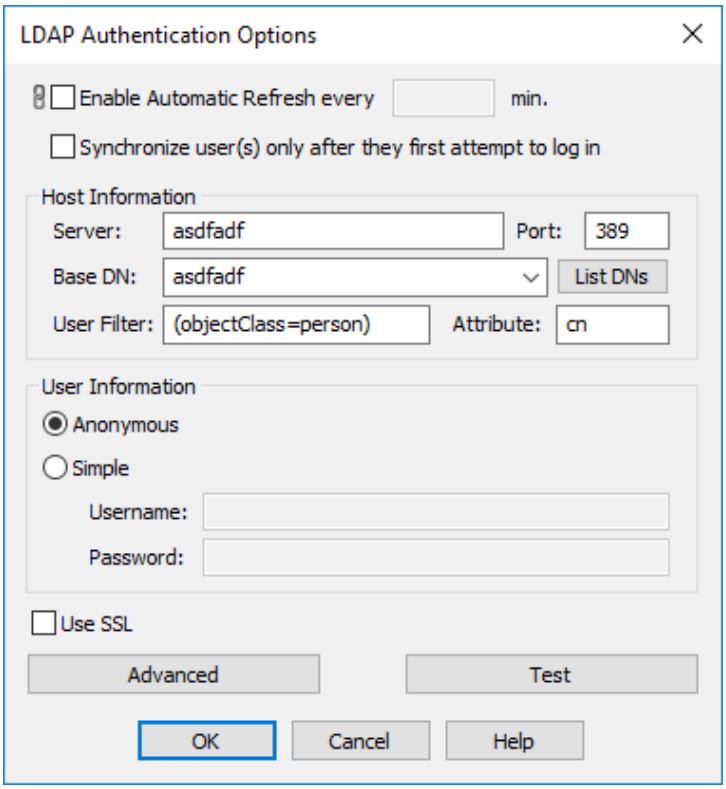
When you use LDAP as the authentication method, EFT pulls the user account list and the authentication from the LDAP Server. Group lists, Group membership, VFS Groups, and VFS User permissions are handled by EFT. These permissions must be configured and maintained in the administration interface or through the COM API.

Changing and Testing LDAP Authentication Options

The **LDAP Authentication Options**dialog box is used to edit and test EFT's connection to the LDAP server after you have configured LDAP Authentication.

To edit or test LDAP authentication settings

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the LDAP Site that you want to configure.
3. In the right pane, click the **General**tab.
4. Next to the **User auth manager** box, click **Configure**. The **LDAP Authentication Options** dialog box appears.



5. To specify that the user list is to be updated automatically, select the **Enable Automatic Refresh every** check box, then specify how often you want EFT to check the authentication database for new users. Clear the check box if you do not want the Site's user list to refresh automatically. (This setting is inherited from the Server's General Settings on the Server's **General**tab. **Never refresh user list automatically**is specified by default.)

   The user list is not refreshed automatically when a Site is stopped for Server startup; user database synchronization timer; or administrator changes related to the user database. You can manually refresh the user database by clicking **View > Refresh User Database**on the main menu.

6. Select the **Synchronize users only after they first attempt to log in** check box to specify whether to load the whole LDAP user database into EFT at once or to pull users one-by-one after successful logins.
7. In the **Server**box, type the **Server** name or IP address.
8. In the **Port**box, keep the default port 389 or specify a different port.

   If you are using SSL:

   - LDAPS communication occurs over port TCP 636.
   - LDAPS communication to a global catalog server occurs over TCP 3269.

- When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged.
- LDAP over SSL must be enabled to effectively change your password via WTC.

9. In the **Base DN**box, type the base domain name for the LDAP user database, in the format `option=value`(e.g.: `dc=forest,dc=tree,dc=branch`), or click **List DNs** to complete the box automatically or select from a list.
10. In the **User Filter**box, type the search filter information. Refer to Advanced LDAP Filtering for a detailed explanation of LDAP filtering. For example:

    ```
    (&(memberof=CN=eft users,cn=Users,dc=demo,dc=vm)
    (objectclass=person))
    (&(memberof=CN=eft users,cn=Users,dc=forest,dc=tree)
    (objectclass=person))
    ```

11. In the **Attribute**box, type a comma-separated list of attributes to retrieve. For example, type:

    ```
    userPrincipalName,mail,email,name,cn
    ```

    (Add `userprincipalname`to the attributes so that the `userprincipalname` is used for the account name in queries.)

12. In the **User Information**area, click one of the following binding methods to define how the client is authenticated:
    - **Anonymous**
    - **Simple**requires a username and password. Note that the username must follow the syntax for the LDAP server that includes the Common Name and the Domain Components of your LDAP server's distinguished name. For example, the username might be the following:

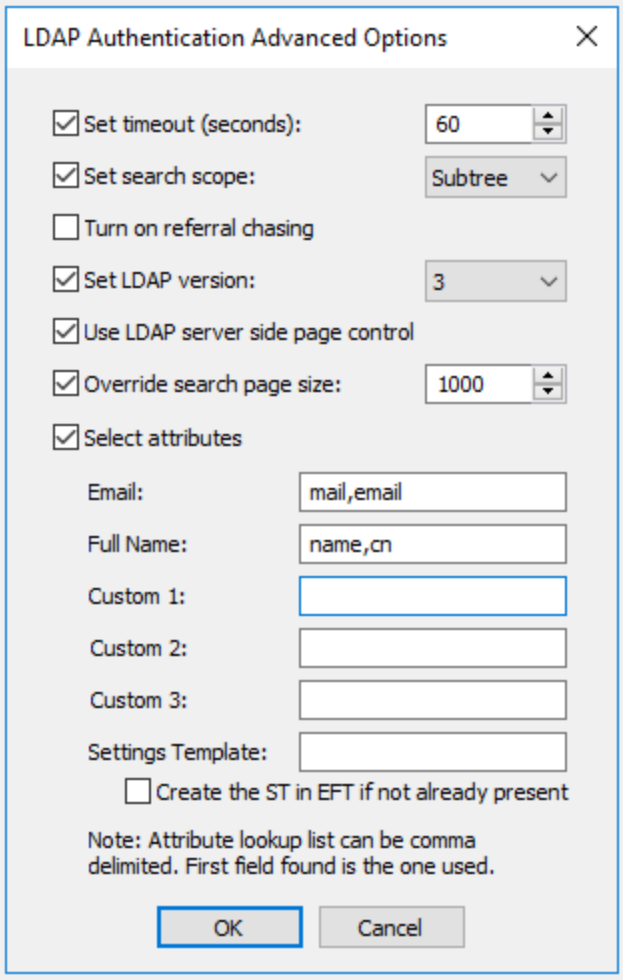
    ```
    cn=Manager,dc=forest,dc=tree,dc=branch
    ```

    For details of creating complex LDAP filters, refer to Advanced LDAP Filtering.

13. If you are using SSL, select the **Use SSL**check box.

    You need to have a certificate that includes Server Authentication on the LDAP server you are connecting to. If you install Certificate Services on the domain on which EFT is installed, you can request the certificate on the LDAP server. For more information, refer to the Microsoft Support article "How to enable LDAP over SSL with a third-party certification authority."

14. To change the advanced options (SSL, timeout, scope, etc.), click **Advanced** and specify advanced options based on your requirements.



- **Set timeoutfor both search/auth** - Specify the connection/query and authentication timeout (in seconds). This option coupled with paging can help you avoid timeouts when querying against large directories. The default is 60 seconds.
- **Set search scope**- This specifies the depth of the level to search for under **BaseDN**.
  - **BASE**- Only the requested object specified in **BaseDN**is searched.
  - **OneLevel**- All of the objects just below this object are searched.
  - **Subtree -**Searches for all the objects within the specified **BaseDN** object recursively.
- **Turn on referral chasing** - If you have referral chasing on, the query returns information for objects that exist in the LDAP structure, but do not actually exist on EFT to which you are connected. The query displays

bookmarks to entries that exist elsewhere in the network that EFT knows about.

- **Set LDAP Version**- LDAP 2 is widely supported and adds anonymous binding and some filtering. LDAP 3 extends the features of LDAP 2 by adding paging (server side) and more complex filtering.
- **Use LDAP server-side page control** - Asks EFT to limit result sets (or pages) to 1000 at a time or the value specified under **Override search page size**, if checked. If **Use server page control** is not selected, client-side paging is used to mitigate timeouts when retrieving large directory listings.

  If you are connecting to a SUN Directory LDAP server, turn off page control. See more information at Using Sun Directory LDAP Server.

- **Override search page size** - Overrides the default page size (1000) for client or server-side page limits. Making the value too large can cause timeouts. Setting the page size too small reduces the overall efficiency.
- **Select attributes**- Returns only the specified attributes for the user objects found as part of the search query. Specifying only necessary attributes will greatly increase the efficiency of your query (since the filtering occurs on EFT side). Add `userprincipalname`to the LDAP query so that the `userprincipalname`is used for the account name in queries.
- For details of specifying **Custom**attributes, refer to Allow LDAP Authentication through DMZ.
- **Settings Template**- Provide the Settings Template name for these users; select the **Create ST in EFT if not already present** check box.

15. To test your settings, click **Test**. The query returns information about your LDAP connection.
16. To close the dialog box, click the **X**in the upper right corner or press ESC.
17. Click **OK** to close the **LDAP Authentication Options**dialog box.
18. Click **Apply**to save the changes on EFT.

User Home Folders on an LDAP-Authenticated Site

The user's home folder location and name is dependent on the **Automatically create home folder** check box in the **Site Setup** wizard and the **ST home folder**defined on the **General** tab of the Settings Template. The table below describes what the user's home folder name and location would be, based on the dependent settings.

"Automatically create home folder" check box in Site Setup wizard	Settings Template Home folder	Client home folder		
		Before login	After first login	Actual home folder
☑ Selected	Not Defined	Undefined	/Usr/JDoe	/>Usr/JDoe
	/Usr/MyUsers	Undefined	/Usr/MyUsers/JDoe	/Usr/>MyUsers/JDoe
☐ Cleared	Not Defined	Undefined	Undefined	Site root
	/Usr/MyUsers	Undefined	Undefined	Settings Template folder

For details of the Virtual File System (VFS), refer to Virtual File System.

Removing Inactive LDAP Accounts from EFT

EFT can remove or disable inactive accounts after a certain number of days of inactivity. On an LDAP site, you can remove inactive users from being displayed in EFT, but they are not removed from the LDAP server. If the user logs in again, then the account will again be displayed in EFT.

Using Sun Directory LDAP Server

Refer to the Globalscape Knowledgebase topic #10218 for information about using Sun Directory LDAP Server.

ODBC Authentication

The topics below provide information about ODBC authentication in EFT.

- Using a DSN-Less Connection with ODBC Authentication
- Changing ODBC Authentication Options
- Creating Tables for your ODBC Data Source
- Script for Creating Necessary ODBC Tables
- User Home Folders on an ODBC-Authenticated Site
- Using an ODBC Data Source for User Authentication
- Allow Server to Accept ODBC Database Passwords that are MD5 Hashed

Using a DSN-Less Connection with ODBC Authentication

You can use a *DSN-less* connection to create an ODBC connection between EFT and the database, using a *connection string*. Connections made in this way are called DSN-less, because they do not require the system administrator to create an ODBC DSN. Rather than relying on information stored in a file, DSN-less connections specify the driver name, and all driver-specific information in the connection string. The connection strings described below combine all the information EFT needs to connect to the database. If you have several simultaneous database connections, a DSN-less connection may be slightly faster than a DSN connection; however, a DSN-less connection is hard-coded to use a certain driver, user identity, and network location, and needs to be updated when the database parameters change.

MDAC version 2.7 or higher must be installed to use a DSN-less connection.

> **NOTE:** If you are upgrading to EFT v8 and using an ODBC database, please contact Globalscape Support. The ODBC schema has changed and you will need to consult with Support so we can assist with the manual process necessary to get it up and running.

To create a Site with a DSN-less connection

1. Follow the procedure in Changing ODBC Authentication Options.
2. In the **Authentication Provider Options** dialog box, type the connection string per the Examples below.

To create the string for a DSN-less connection

1. On a remote SQL Server, create an ODBC database, login, etc.
2. Create a (system) DSN for the server and verify that it works.
3. In EFT configure the ODBC pre-populated string with the correct information.

Be sure to use the correct driver for your database. Create a connection string as described below and type it into the **Authentication Provider Options** dialog box. The connection string includes the name of the driver you need for your database, the location of your database, the name of your database, and, if necessary, a user name and password to access the database. Connection strings are lists of keywords and associated values; each keyword identifies a particular connection attribute.

For local databases, the connection string must include:

- Provider [Provider=]
- Driver [DRIVER=]
- Database path and name, including the file extension [Dbq=]

- Username [Uid] and Password [Pwd] are required only if the database is password protected

For remote databases, your connection string must include:

- Driver [DRIVER=]
- Server [SERVER]
- Database [DATABASE]
- Username [UID]
- Password [PWD]

Examples:

```
DRIVER={SQL
Server};Provider=MSDASQL;SERVER=192.168.100.242;DATABASE=dsh_
odbc;UID=sa;PWD=canada
            DRIVER={SQL
Server};Provider=MSDASQL;server=eft1;database=eftdb;trusted_
connection=yes
```

If you have a remote MYSQL database named **Example** your connection string is:

```
Provider=MSDASQL;DRIVER={MySQL ODBC 3.51
Driver};SERVER=10.10.10.1;DATABASE=Example;UID=myusername;PWD=m
ypassword
```

Of course, use the database Server IP, database name, user ID, and password needed to connect to the database.

If you are connecting to a database server through ODBC, the server's configuration determines whether it is case-sensitive. Check with your database server administrator to determine whether your server is configured as case-sensitive. If your database is case-sensitive, you will have to edit the tables accordingly.

Do not put any line breaks in your connection strings.

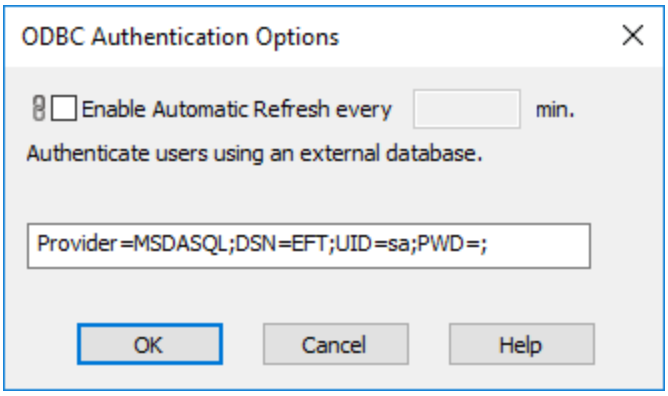
With some installations, you may need to add a pointer to a Microsoft Access workgroup file as well as the username and password. A default installation of Access does not require this.

Changing ODBC Authentication Options

When you create a Site, you specify the user database authentication method. You cannot change the authentication *method* after you have created a Site, however, if you need to change the authentication *options*, you can do so from the **Site Options** tab. The options available in the **Authentication Provider Options** dialog box change depending on which authentication method the Site uses.

To edit the authentication options for a Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. In the right pane, click the **General** tab.
4. Next to the **User auth manager** box, click **Configure**. The **Authentication Provider Options** dialog box appears.



5. To specify that the user list is to be updated automatically, select the **Enable Automatic Refresh every** check box, then specify how often you want EFT to check the authentication database for new users. Clear the check box if you do not want the Site's user list to refresh automatically.
6. The user database is not refreshed automatically when a Site is stopped for Server startup; user database synchronization timer; or administrator changes related to the user database. You can manually refresh the user database by clicking **View > Refresh User Database** on the main menu.

   In the text box, edit the connection string, as needed. Refer to Using a DSN-Less Connection with ODBC Authentication for details of how to create a connection string depending on the type of database to which you are connecting.

7. Click **OK** to close the dialog box.
8. Click **Apply** to save the changes on EFT.

Creating Tables for Your ODBC Data Source

When upgrading from 7.4.x to 8.0.x, the ODBC schema has changed. If you are using ODBC as the authentication database, then you will need to consult with Globalscape Support so we can assist with the manual process necessary to get EFT updated and running.

The ODBC authentication database needs to have TLS 1.0, 1.1 enabled for connection to complete. These are disabled by default.

You must create two tables in the database for your data source. Scripts are provided that will create the necessary tables.

If users receive an error saying they are not logged in, make sure the "anonymous" row in the "ftpserver_users" table is set to "0" or "1"; it cannot be set to "Null".

The **ftpserver_users**table lists the user accounts and permissions groups in the Site. A user account uses the information from all fields. A permission group uses only the ID, Name, and Description fields and is used only for organizational purposes, not as a user login.

Field Name	Data Type	Field Size	Description
ID (Primary Key)	AutoNumber	Long Integer	User ID
NAME	Text	50	Login name for this user
PASSWORD	Text	200	Password for this user (Stored in clear text; SHA-256 encrypted, if enabled; or optionally, using MD5.)
DESCRIPTION	Text	200	Description for this user
TYPE	Number	Integer	0=Group, 1=User
PASSWORD_TYPE	Number	Integer	Standard, OTP_MD4, OTP_MD5: Differentiates Regular vs. SKEY (OTP) password type. • 0 = Standard Password • 1 = MD4 OTP • 2 = MD5 OTP
MD_ITER	Number	Long Integer	Current MDX iteration - used by OTP accounts only
OTP_SEED	Text	16	OTP Seed to be used for MDX Passwords - used by OTP accounts only.

Field Name	Data Type	Field Size	Description
ANONYMOUS	Number	Long Integer	0=Normal Password, 1=Any password
ANONYMOUS_ EMAIL	Number	Long Integer	0=Any anonymous password, 1=email password required
FULLNAME	Text	200	User's full name
EMAIL	Text	200	User's email address
PHONE	Text	200	User's phone number
PAGER	Text	200	User's pager number
FAX	Text	200	User's fax number
COMMENTS	Text	200	User comments
ENABLED	Number	Integer	0 = Account disabled 1 = Account enabled -2 = Inherited
HOMEDIRECTORY	Text	512	Legacy field no longer used, but must be present in the database.
SETTINGSLEVEL	Text	200	Name of user's Settings Template.
COMPANY	Text	200	Name of user's company
MOBILE	Text	200	User's mobile phone number
DUNS	Text	200	User's/Company's DUNS number
PARTNER_ID	Text	200	User's partner ID
CUSTOM1	Text	200	Custom field defined by administrator (for example, for employee number, building number, additional phone number)
CUSTOM2	Text	200	Custom field defined by administrator (for example, for employee number, building number, additional phone number)
CUSTOM3	Text	200	Custom field defined by administrator (for example, for employee number, building number, additional phone number)

The **ftpserver_ids**organizes users into "groups" of permission levels. For each permission Group to which a user belongs there should be one entry in the table below.

Field Name	Data Type	Field Size	Description
ID	AutoNumber	Long Integer	Unique ID for the record (key field).
USER_ID	Number	Long Integer	This value refers to a user record in the ftpserver_users table. A corresponding ftpserver_users record (where ftpserver_ids.User_ID = ftpserver_users.ID) must exist with Type= 1.
Group_ID	Number	Long Integer	This value refers to the Settings Template to which the User_ID user record belongs. A corresponding ftpserver_users record (where ftpserver_ids.Group_ID = ftpserver_users.ID) must exist with Type= 0.

Script for Creating Necessary ODBC Tables

When upgrading from 7.4.x to 8.0.x, the ODBC schema has changed. If you are using ODBC as the authentication database, then you will need to consult with Globalscape Support so we can assist with the manual process necessary to get EFT updated and running.

Related Topics

- EFT Database Utility
- Command-Line Parameters
- Database User Account Privileges
- Manually Creating the ARM Database in SQL Server
- Manually Creating the ARM Database in Oracle

User Home Folders on an ODBC-Authenticated Site

The user's home folder location and name is dependent on the **Automatically create home folder** check box in the Site Setup wizard and the Settings Template home folder definition on the **General**tab of the Site. The table below describes what the user's home folder name and location would be, based on the dependent settings.

Settings Template home folder	Client home folder		
	Before login	Client Settings	Actual home folder
Not Defined	/Usr/JDoe	/Usr/JDoe	/Usr/JDoe
/Usr/MyUsers	/Usr/MyUsers/JDoe	/Usr/MyUsers/JDoe	/Usr/MyUsers/JDoe

For details of the Virtual File System (VFS), refer to Virtual File System.

Using an ODBC Data Source for User Authentication

EFT allows you to use any ODBC-compatible database as a source for user authentication. You may add and remove users and set certain permissions using your existing database utility or in the administration interface. EFT uses ADO to communicate with the authentication databases using "generic" SQL statements.

You do NOT have to use DSN for ODBC authentication. Refer to Using a DSN-Less Connection with ODBC Authentication for details.

If you are configuring a DSN on a 64-bit Windows system, you need to run the 32-bit version of the Windows “ODBC Database Source administrator” application. EFT cannot see DSNs created using the 64-bit version, which is the one that will be launched from the Windows Control Panel on 64-bit Windows Operating Systems. When configuring a DSN on a 64-bit Windows System, run the 32-bit version, usually **C:\Windows\SysWOW64\odbcad32.exe**.

To use an external ODBC data source you must:

- Create tables in an ODBC data source
- Establish a System Data Source Name (DSN) in the ODBC Source administration tool
- Configure EFT to use the System DSN
- Install Microsoft Data Access Components (MDAC) 2.6 or higher
- (SQL Server only) The DSNs must be configured to use SQL Server authentication if EFT is running as Local System
- (SQL Server only) SQL Server Native Client Driver must be used for IPv6 connectivity.

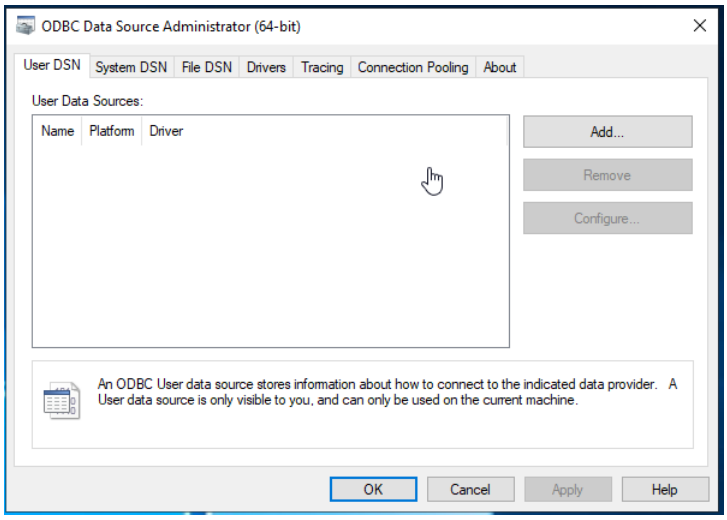
Establishing a System Data Source Name (DSN)

After you have created your database, you must associate it with your system by establishing a Data Source Name (DSN). A DSN is a data structure that contains the information about a database that an Open Database Connectivity (ODBC) driver needs to connect to it, such as the name, directory, and driver of the database, and the ID and password of the user.

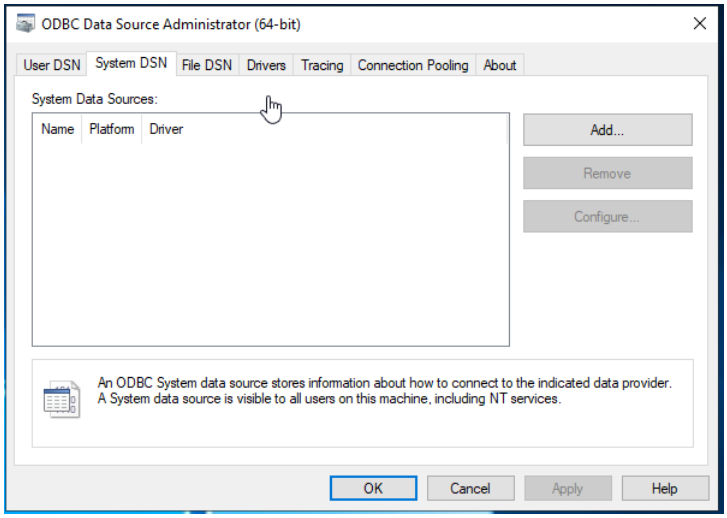
To use a DSN-less connection with ODBC authentication, refer to Using a DSN-Less Connection with ODBC Authentication.

To establish a system DSN

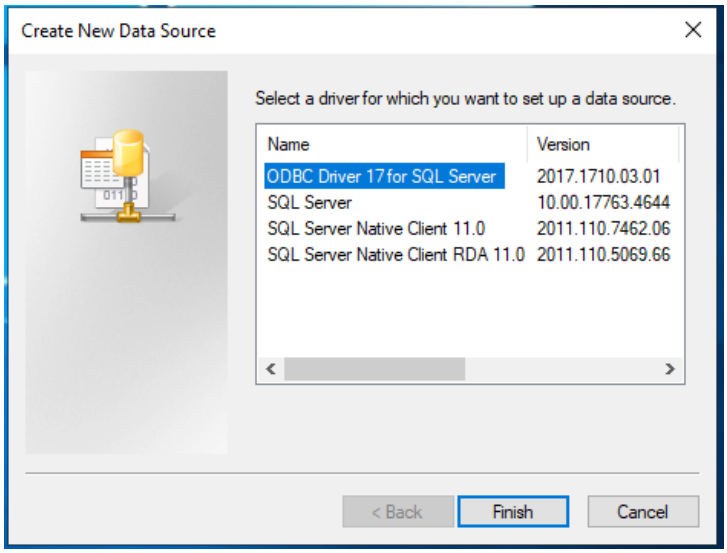
1. In Windows, click **Control Panel**, **administrative Tools >Data Sources (ODBC)**. The **ODBC Data Source Administrator** appears.



2. Click the **System DSN** tab.



3. Click **Add**. The **Create New Data Source** dialog box appears.



4. Click the database driver that corresponds with the database type to which you are connecting, and then click **Finish**.
5. In the dialog box that appears (differs depending on driver selected), type the **Data Source Name** and **Description**. The default DSN is EFT.
6. Click **Select** to specify the database file to use, and then click **OK**.
7. Click **OK** to close all of the dialog boxes and save the changes.

Allow Server to Accept ODBC Database Passwords that are MD5 Hashed

Refer to the Globalscape Knowledgebase topic #10537 for information about using MD5 hashed ODBC database passwords.

EFT Logging and Visibility

The topics below describe EFT logging and visibility functions.

- EFT Transfer Activity Logging
- EFT Client Activity Logging
- Event Rules Client Logging
- EFT Server Activity Logging
- Installation Logging
- Viewing Connections to a Site
- Viewing Server Statistics
- Viewing Site Statistics
- Viewing Transfers To and From the Site
- Performance Counters

EFT Transfer Activity Logging

As the EFT log file subsystem writes out the date for the log, it compares the current computer date/time to the value for the log rotation (hourly/daily/weekly/monthly/yearly) period specified on the logs tab of the Server. When a write-to-log operation occurs that is calculated to cross a period (that is, the prior write was within a former period, but the current date/time at write is a new period), EFT rotates the log file name and then writes to that new log.

EFT activities can be logged in various places.

- The **EFT<servername>.log** file is the root logger and controls all logging items as defined in logging.cfg. Individual loggers can be enabled and increased in verbosity as needed. Some loggers contain sub appenders to log specific aspects.
- For information about the Audit Database logs, refer to Auditing Database Errors and Logging. (Not to be confused with Audit Database Settings.)
- For event rule logging (such as *cl060312.log*) refer to Event Rules Client Log.
- For installation logs, refer to Installation Logging.
- For DMZ Gateway logging, refer to DMZ Gateway Logging.
- For Windows Event Logs, refer to Windows Event Log (WEL) Action.

EFT Client Activity Log

To monitor EFT client activity, you can reference EFT's log files, including registration state of modules, server/site functions, SFTP, SSL/TLS connections, and of course, errors and warnings.

- The EFT client activity log, also known as "TED6" logs, is used to log client connection information (event rules and outbound transfers), client commands/requests, remote server responses, and status messages.
- EFT client log files are saved in the **C:\ProgramData\Globalscape\EFT Server\Logs** folder.
- See also Event Rules Client Log.

Event Rules Client Log

When EFT's **Download** and **Copy/Move** Action offloads or downloads files, the outbound session is recorded to a log file that is named **cl[yymmdd].log** (for example, **cl060312.log**) and saved in the EFT installation folder (**C:\ProgramData\Globalscape\EFT Server\Logs**). The log file is formatted as follows:

> Time; Protocol; Host Name:Port; User Name; Local Path; Remote Path; Operation; GetLastCode

For example:

```
2006-03-06 10:11:03; ftp; 192.168.20.171:21; ClientA;
 C:\test1.txt; /test1.txt; download; 226;
```

A tenth column can be added to the CL log by defining an advanced property. Refer to https://kb.globalscape.com/KnowledgebaseArticle10262.aspxfor details.

The log can be used for troubleshooting connection and transfer errors. The "GetLastCode" value returns the protocol success or error code or socket error. For example, trying to connect to a non-existent website will result in the socket error code 10060, *connection timeout*. For example, if EFT was unable to make a connection to a remote host, a code that could appear in the cl log is 10061 (connection refused). If you are using FTP to make the connection and upload/download a file, you will also see FTP Status and Error Codes. Refer to "Windows Sockets Error Codes" in the Microsoft Developer Network for a complete list of common socket error codes.

In addition to the standard socket error codes, EFT defines the socket error codes described below.

#	Description
0	Success (connected OK)
1	General socks failure
2	Socket connection not allowed by ruleset
3	The network is unreachable
4	The host is unreachable
5	The remote server actively refused the connection
6	The Time To Live (TTL) expired. This could indicate a network problem.
7	The command was not supported by the remote host. Also a catchall error code.
8	The address type or format is not supported
10	Illegal socks name
11	Socks5 authentication failure (username/password incorrect)
12	Can't connect to socks server
2000	Internal timeout error code (multiple reasons, such as firewall blocking connection, etc.)

FTP and **FTP over SSL** only return protocol-level success and error codes. For example, a successful transfer would return 226 or a bad login password would return 530. Refer to RFC 959 for a complete list of FTP/S return codes.

SFTP (SSH2) returns the following success and error codes:

#	Description
-1	Undefined or unknown error (not enough information to determine exactly why it failed) When an OpenSSH client disconnects from EFT, it reports that the exit status is **-1**. The default return code is -1, unless an optional message is returned from the server. EFT does not return the optional message, so the exit status is always -1.
0	The operation completed successfully
1	The operation failed because of trying to read at end of file
2	The requested file does not exist
3	Insufficient privileges to perform the operation
4	The requested operation failed for some other reason
5	A badly formatted message was received. This indicates an error or incompatibility in the protocol implementation
6	Connection has not been established (yet) and a timeout occurred

#	Description
7	Connection to the server was lost, and the operation could not be performed
8	A timeout occurred

Related Topics

- Introduction to EFT Logging
- Log Format, Type, and Location
- EFT in the Windows Event Viewer

EFT Server Activity Log

To monitor EFT activity, you can reference EFT's log files. EFT supports W3C, Microsoft IIS, and NCSA log file formats. Server events are logged to a file named *[log file format]yymmdd.log*, where YY, MM, and DD indicate the numeric year, month, and day respectively. Depending on the log file format selected, a 2-letter abbreviation is prepended to the filename, as described in the table below. For example, a log file in the Microsoft IIS format created on August 22, 2024 is named `in240822.log`.

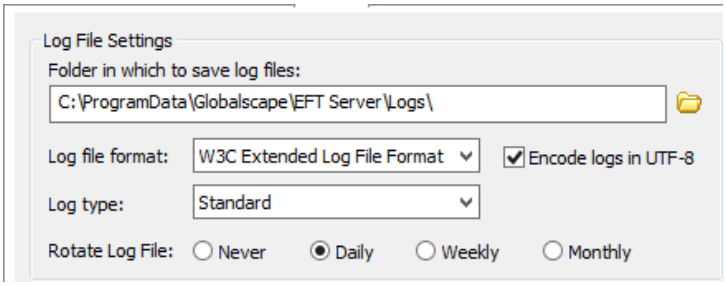
By default, log files are saved in the EFT data directory in the **Log** folder (for example, **C:\ProgramData\Globalscape\EFT Server\Logs**). Outbound connection information is audited in that same folder in a log named cl<date>.log.

When using HA, you need to specify a unique location (local) for the log files. This is for troubleshooting purposes (to know what node an issue occurred on). Also, having two nodes write to the same file causes issues with file locking, which will cause data in the logs to be lost.

Log Format, Type, and Location

To specify log settings

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node.
3. In the right pane, click the **Logs**tab.



4. In the **Log File Settings**area, in the **Folder in which to save log files** box, type the path to the directory in which to save this Server's log files. To browse for a path, click the folder icon .
5. In the **Log file format** list, click **W3C Extended**, **Microsoft IIS**, **NCSA Common**, or **No Logging**. Changing the log file format disconnects all active users. It is recommended to stop all Sites or wait until all users are inactive before changing the log file format. The W3C format records all times in GMT (Greenwich Mean Time).

6. Clear the **Encode logs in UTF-8** check box if you do not want to encode logs in UTF-8 format. When the check box is cleared, the **u_ex*.log**file is named **ex*.log**.

   From Microsoft TechNet:

   When using the UTF-8 logging feature, note the following:

   - A log file logged in UTF-8 does not contain a Byte Order Mark (BOM). File editors use this mark to identify text as UTF-8 text. Therefore, if you attempt to open a log file that is logged in UTF-8 in Notepad by double-clicking the file or by using the Open With option, the file might not display correctly. To open the file in a way that displays it correctly, use the Open command on the File menu and then select UTF-8 in the Encoding box.
   - UTF-8 is a double-byte character-set standard. ASCII is a single-byte character-set standard. Because of this disparity, logging UTF-8 information to an ASCII file causes a ? to be logged for the characters that cannot be converted to the code page of the server.
7. In the **Log type**list, click **Standard** or **Verbose**. (Verbose provides more details, but makes larger files.)
8. In the **Rotate Log File** area, specify **Never**, **Daily**, **Weekly**, or **Monthly**.
9. Click **Apply** to save the changes on EFT.
10. Stop and restart EFT.

For information about the Audit Database Settings, refer to Auditing Database Errors and Logging.

Log File Format	Abbreviation
W3C	ex
NCSA	nc
Microsoft IIS	in

Log Example

Below is an example of an **ex**-formatted log:

```
#Version: 1.0
#Software: CuteLogger
#Date: 2010-04-08 20:07:50
#Fields: date time c-ip c-port cs-username cs-method
cs-uri-stem cs-uri-query sc-status sc-bytes cs-bytes s-name s-
port
2010-04-08 20:07:07 192.168.241.1 - test [1]user test - 331 - -
- 22
```

```
2010-04-08 20:07:07 192.168.241.1 - test [1]pass ******* - 230 -
- - 22
2010-04-08 20:07:16 192.168.241.1 - test [1]created
/Test+File+1.txt - 226 - 54 - 22
2010-04-08 20:08:23 192.168.241.1 - test [1]rnfr
/Test+File+1.txt - 350 - - - 22
2010-04-08 20:08:23 192.168.241.1 - test [1]rnto
/Test+File+2.txt - 250 - - - 22
2010-04-08 20:08:26 192.168.241.1 - test [1]sent
/Test+File+2.txt - 226 - 54 - 22
2010-04-08 20:10:02 192.168.241.1 - test [1]dele
/Test+File+2.txt - 250 - - - 22
2010-04-08 20:10:08 192.168.241.1 - test [1]ssh_disconnect
timeout - 421 - - - 22
2010-04-08 20:10:09 192.168.241.1 - test [1]ssh_disconnect
timeout - 421 - - - 22
2010-04-08 20:11:57 192.168.241.1 - test [2]user test - 331 - -
- 990
2010-04-08 20:11:57 192.168.241.1 - test [2]pass ****** - 230 -
- - 990
2010-04-08 20:12:04 192.168.241.1 - test [2]created
/Test+File+1.txt - 226 - 54 - 990
2010-04-08 20:12:16 192.168.241.1 - test [2]rnfr
/Test+File+1.txt - 350 - - - 990
2010-04-08 20:12:16 192.168.241.1 - test [2]rnto
/Test+File+2.txt - 250 - - - 990
2010-04-08 20:12:28 192.168.241.1 - test [2]rnfr
/Test+File+2.txt - 350 - - - 990
2010-04-08 20:12:28 192.168.241.1 - test [2]rnto
/Test+File+3.txt - 250 - - - 990
2010-04-08 20:12:31 192.168.241.1 - test [2]sent
/Test+File+3.txt - 226 122 - - 990
```

The log can be read as described below:

Field	Description	Example
(Each field in the log has either a value (for example, date) or a dash (-) if no value was sent for that field.)		
date	Date log was recorded	2010-04-08
time	Time log was recorded	20:07:16
c-ip	Client IP address	192.168.241.1
c-port	Client port	21
cs-username	Username	test

Field	Description	Example	
cs-method	Method (Command Sent)	ABOR	Abort an active file transfer
		ACCT	Account information
		ALLO	Allocate sufficient disk space to receive a file
		APPE	Append
		AUTH	Authentication/Security Mechanism
		CCC	Clear Command Channel
		CDUP	Change to Parent Directory
		CHANGEPASSWORD	Change the password
		CLIENTCERT	Client SSL certificate was rejected (reason is provided in the log entry).
		COMB	Combines file segments into a single file on EFT.
		CREATED	File was created (uploaded).
		CWD	Change working directory
		DELE	Delete file
		EPRT	Specifies an extended address and port to which the server should connect
		EPSV	Enter extended passive mode
		FEAT	Get the feature list implemented by the server
		HELP	Display a list of all available FTP commands
		KICK	Client connection was closed by administrator.

Field	Description	Example	
		LIST	Returns information of a file or directory if specified, else information of the current working directory is returned
		MDTM	Return the last-modified time of a specified file
		MKD	Make directory
		MLSD	Lists the contents of a directory if a directory is named
		MLST	Provides data about exactly the object named on its command line, and no others
		MODE	Sets the transfer mode (Stream, Block, or Compressed)
		NLIST	Returns a list of file names in a specified directory
		NOOP	No operation (dummy packet; used mostly on keepalives)
		OPTS	Select options for a feature
		PASS	Authentication password
		PASV	Enter passive mode
		PBSZ	Protection Buffer Size
		PORT	Specifies the port to which the server should connect
		PROT	Data Channel Protection Level
		PWD	Print working directory Returns the current directory of the host
		QUIT	Disconnect

Field	Description	Example
		REIN — Re initializes the connection REST — Restart transfer from the specified point RETR — Transfer a copy of the file RMD — Remove a directory RNFR — Rename from RNTO — Rename to SENT — File was sent (downloaded). SITE — Sends site specific commands to remote server SIZE — Return the size of a file SMNT — Mount file structure SSCN — Set secured client negotiation SSH_DISCONNECT — SFTP (SSH) client connection was closed (reason is provided in the log entry). STAT — Returns the status STOR — Accept the data and to store the data as a file at the server site STOU — Store file uniquely STRU — Set file transfer structure SYST — Return system type TYPE — Sets the transfer mode USER — Authentication username WEBSERVICE — Web Service was invoked. XCRC — Compute CRC32 checksum on specified file
cs-uri-stem	Stem portion of URI	/Test+File+1.txt
cs-uri-query	Query portion of URI	-

Field	Description	Example
sc-status	Status code	226 (Closing data connection. Requested file action successful.)
sc-bytes	The number of bytes that the server sent to the client.	541
cs-bytes	The number of bytes that the client sent to the server.	54
s-name		-
s-port	Server port	22

Installation Logging

The installation log file is intended for debugging purposes and contains messages that may help resolve issues that arise during installation.

- During installation and maintenance, the installer creates an **Installer.log** file in the **%TEMP%\<Product Name>**directory. For example:
  - **C:\Users\administrator\AppData\Local\Temp\EFT Server\Installer.log**
  - **C:\Users\administrator\AppData\Local\Temp\EFT Server\Installer.log**
- At the completion of the installation, either due to success or failure, the installer copies the final log to the **<InstallDir>\logs** directory, if it exists. If the installer fails during an initial clean installation, the **<InstallDir>\logs**directory may not exist. In this case, the final log file remains in the **%TEMP%\<Product Name>**directory.
- The installer attempts to append to the existing log file on subsequent runs of the installer (for example, if the user performs a Reinstall). It does this by copying any existing **Installer.log**file from the installation directory into the Temp directory, writing to it during installation, and then copying it back to the **<InstallDir>\logs**directory when the installation is finished.
- You can write out the same log messages to another log file of your choosing using the **/logfile=<Log file>** command line switch to the installer.

Debug Logging

The installer is capable of writing the same messages that go to the Main Installer Log using the Windows debug logging infrastructure. These messages may be viewed using a utility such as SysInternal's DebugView application. To enable this logging, the installer must be run from the command line with the **/debug** switch.

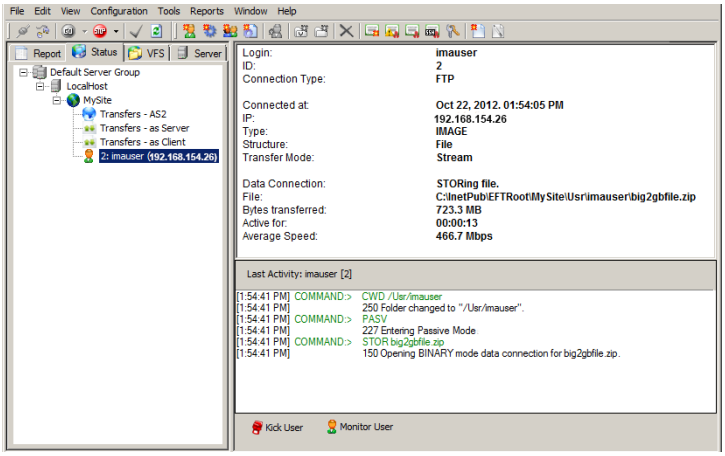
Viewing Connections to a Site

On the Status tab, expand the **Site** node to view connection status for the Site, AS2 transactions, and each connected user account.

For example, if a user is connected to EFT via SFTP, the Site tree displays an ID number, the username, the IP address of the Site, and "SFTP." For example, **4: jbite (192.168.174.235) - SFTP**. The right pane displays the Login (username), ID, Connection Type, date and time connected, IP address, Average Upload Speed, and Average Download Speed. The bottom of the right pane displays the connection log.

You can forcibly disconnect a user by selecting the user in the tree, and then clicking **Kick User** in the right pane.

You can see more details of the user's activity by selecting the user in the tree then clicking **Monitor User** in the right pane.

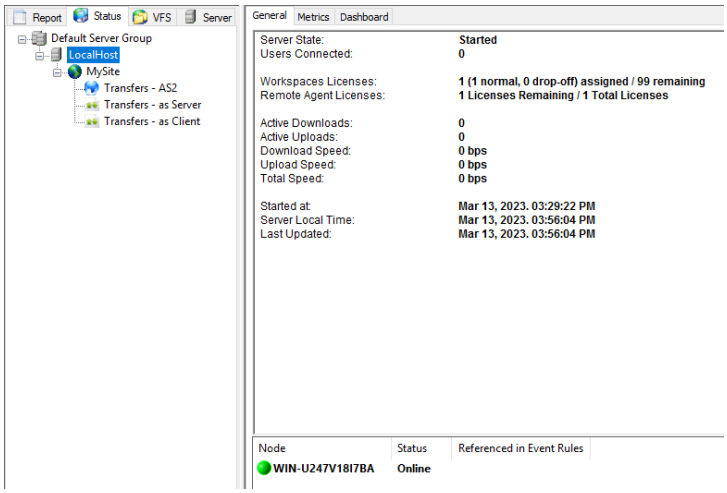


Viewing Server or Node Status

In the administration interface, you can view the status of EFT in real time, such as number of users connected, average speed, and so on. You can view Server status on the **Status** tab or on the Server node's **General**tab.

To view status on the Statustab

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Status**tab, click the **Server** node. EFT's statistics appear in the right pane.



3. In an HA cluster, you can see the nodes and their status at the bottom of the **Status**viewer.
    - **Online**: EFT server service is up and communicating via Heartbeat to the rest of the node in the cluster
    - **Master**: Same status as **Online**, however this node is designated as the **Master**node for Event Rules Load balancing.

Only one node can be show as Master in the list of the nodes from the cluster. This status only is displayed if you have at least one Event Rule enabled and configured to run in more than one node from the cluster. If this status exists, the Master node will create an exclusive file lock onto **MasterNodeLock**file in the HA config shared folder.

- **Offline**: EFT server service is down; no communication via Heartbeat is performed
- **Unknown**: A node name is being reference in at least one Event Rule; however, this node name is not part of the cluster.

To view status on the Server tab

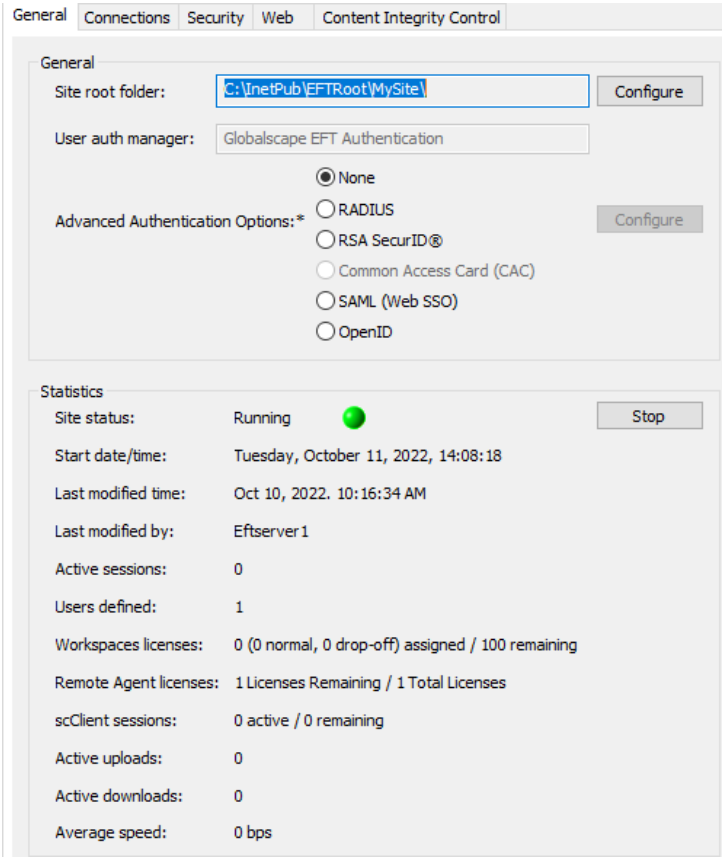
1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Server** node.
3. In the right pane, click the **General**tab. EFT's statistics appear in the right pane.
    - **Server status**: Displays "Service is started" or "Service is stopped." You can also stop and start the EFT service on this tab.
    - **Start date/time**: Displays the date and time that the EFT service was last started.
    - **Uptime**: Displays the length of time that the EFT service has been running since it was last started.
    - **Last modified time**: Displays the date and time that EFT was last modified.
    - **Last modified by**: Displays the username of the user who last modified EFT.
    - **Active sessions**: Displays the number of users who are currently logged in to EFT.
    - **Active uploads**: Displays the number of uploads in progress.
    - **Active downloads**: Displays the number downloads in progress.
    - **Average speed**: Displays the average transfer speed.
    - **Workspaces licenses**: Displays the number of licenses used and number licensed (allowed)
    - **Web clients licenses**: Displays the number of licenses used and number licensed (allowed)

Viewing Site Statistics

In the administration interface, you can view the status of the Site in real time, such as number of users connected, average speed, the number of active Web Transfer Clients sessions, and so on.

To monitor current statistics on the Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Site** that you want to monitor.
3. In the right pane, click the **General**tab.



The Site's information appears in the **Statistics**area.

- **Site status**: Displays "Running" or "Stopped"; you can also stop and start the Site.
- **Start date/time**: Displays the date and time that the Site was last started.
- **Last modified time**: Displays the date and time that the Site was last modified.

- **Last modified by**: Displays the username of the user who last modified the Site.
- **Active sessions**: Displays the number of users who are currently logged in to the Site.
- **Users defined**: Displays the number of user accounts defined on the Site.
- **scClient sessions**: Displays the number of sessions in use and available. (scClient is part of the Accelerate module, which is no longer offered for EFT; however, some customers who upgrade still have Accelerate licenses.)
- **Active uploads**: Displays the number of uploads in progress.
- **Active downloads**: Displays the number downloads in progress.
- **Average speed**: Displays the average transfer speed.

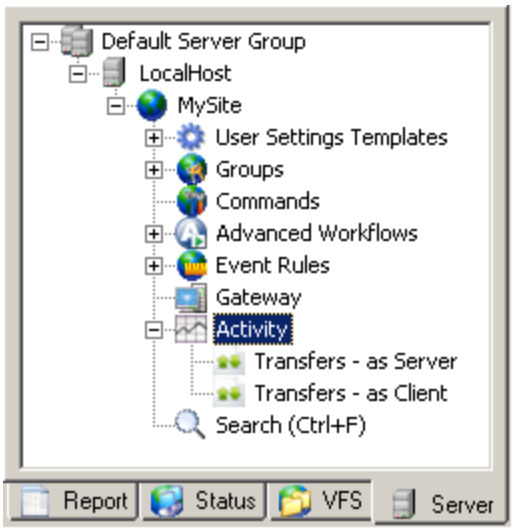
You can view details of transfers to and from EFT on the **Status**tab. Refer to Viewing Transfers To and From a Site for details.

Related Topics

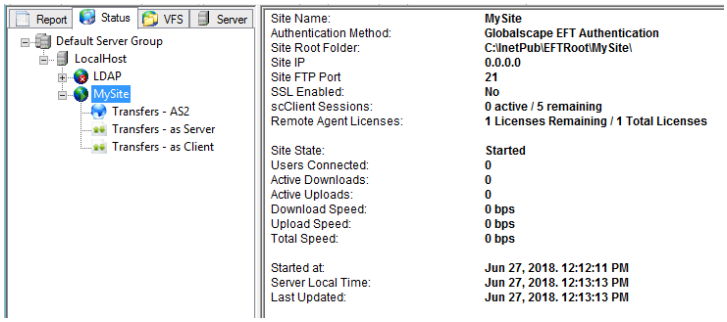
- Forcibly Logging a User Off of EFT
- Viewing Server Statistics
- Viewing Transfers To and From a Site

Viewing Transfers To and From a Site

You can view details of transfers to and from EFT on the **Status**tab. On the **Server** tab, a node in the tree labeled **Activity** has two branches: **Transfers - as Server**and **Transfers - as Client**. Click one of the branches to open the **Status**tab to that view.



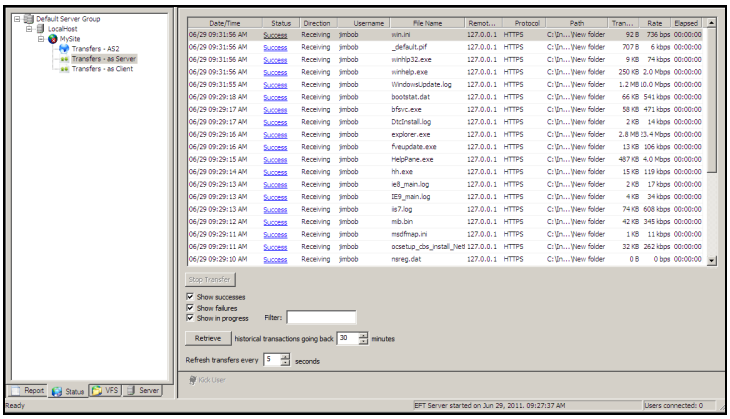
Or just click the Site's **Status**tab:



Then click one of the nodes:

Transfers - as Server - Displays "Receiving" when uploading files to the Web Transfer Client or sharing files via Workspaces.

Transfers - as Client - Displays when you upload files using an FTP client or drag-and-drop into a user folder.

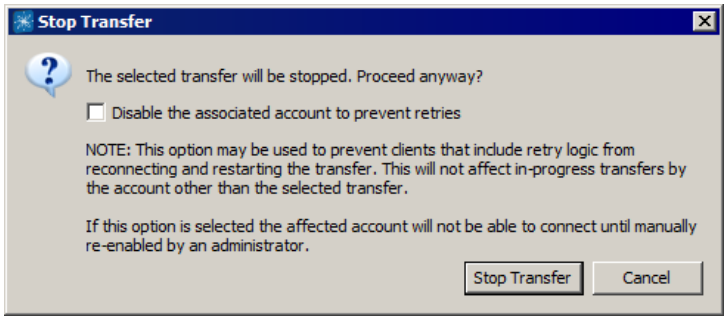


Transfers appear at the top of the window. The Transfer list may not be up to date, depending on the size of transfer, network performance, and so on. Transfers that are small and quickly processed may not appear in the list or are quickly overwritten as others files are processed. If you click **Retrieve**, transfers stored in the database and in-progress transfers will appear in the list.

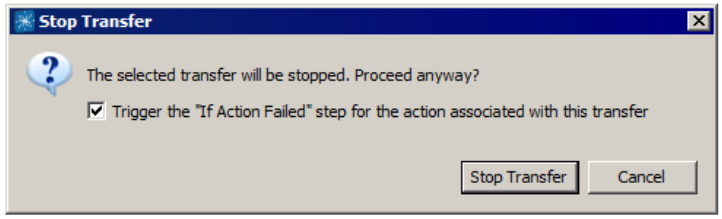
You can:

- Sort data by a column by clicking the column header.
- Filter results by typing characters in the **Filter**box. For example, display only transfers by a particular user or from a specific Remote IP address.
- Display or hide successful, failed, or in progress transfers by selecting or clearing the **Show successes**, **Show failures**, and **Show in progress** check boxes.
- Retrieve historical transactions by specifying the number of minutes (from 1 to 9999) in history that you want to retrieve, then clicking **Retrieve**. The maximum number of records that can be displayed is 10,000.
- Specify which columns to display or hide by right-clicking on the column header, and then clicking the column name to display or hide.
- Click the linked text (Success or Failure) to view the details of the transfer.
- Stop an in-progress transfer by clicking **Stop Transfer**. Stopping the transfer can free up bandwidth when large transfers are occurring and a higher priority transfer needs to get through. You can also select multiple transfers to stop them all at the same time.
    - The Administrator Actions report includes transfers stopped by the administrator, as does other relevant file transfer activity reports.
    - Stopped client transfers will ***not***retry automatically. Other connections from the user are unaffected.

- Stopped outbound transfers are audited to the CL.log; stopped inbound transfers are audited to the EX.log.
- When you click **Stop Transfer**, a prompt appears in which you can choose to disable the user account that initiated the transfer to prevent retries. If disabled, the account must be enabled by an administrator. (You will have to refresh the interface to see that the user is disabled.)



- For client offload Event Rule actions (that is, Copy/Move file Actions), a prompt appears in which you can choose whether to consider the stopped transfer a failed transfer. If you do not want any "If Action Failed" Actions to occur when the transfer is stopped, clear the check box, and then click **Stop Transfer**.



The available columns are listed in the table below.

Column	Description	Transfers as Server	Transfers as Client
Date/Time	Date and time of transfer in the format MM/DD HH:MM:SS AM/PM	x	x
Status	Success or Failed	x	x
Direction	Whether sending or receiving the file	x	x
Username	Username of account initiating the transfer	x	x
File Name	Filename of file being transferred	x	x
Remote IP	IP address of remote computer	x	x
Local IP	Server's IP address	x	n/a

<table>
<tr><th>Column</th><th>Description</th><th>Transfers as Server</th><th>Transfers as Client</th></tr>
<tr><td>Local Port</td><td>Server's port on which the file is transferred</td><td>x</td><td>n/a</td></tr>
<tr><td>Remote Port</td><td>Port of remote computer used for transfer</td><td>n/a</td><td>x</td></tr>
<tr><td>Protocol</td><td>Protocol over which the file is transferred</td><td>x</td><td>x</td></tr>
<tr><td>Path</td><td>Path on EFT to which file is transferred</td><td>x</td><td>n/a</td></tr>
<tr><td>Remote Path</td><td>Remote path of file being transferred</td><td>n/a</td><td>x</td></tr>
<tr><td>Local Path</td><td>Local path of file being transferred</td><td>n/a</td><td>x</td></tr>
<tr><td>Transferred</td><td>Size of file being transferred</td><td>x</td><td>x</td></tr>
<tr><td>% Complete</td><td>Percentage of transfer completed; HTTP/S (both directions), and SFTP, FTP, and FTPS server downloads, and all client (outbound) transfers display % complete; SFTP, FTP, and FTPS inbound cannot display % complete.

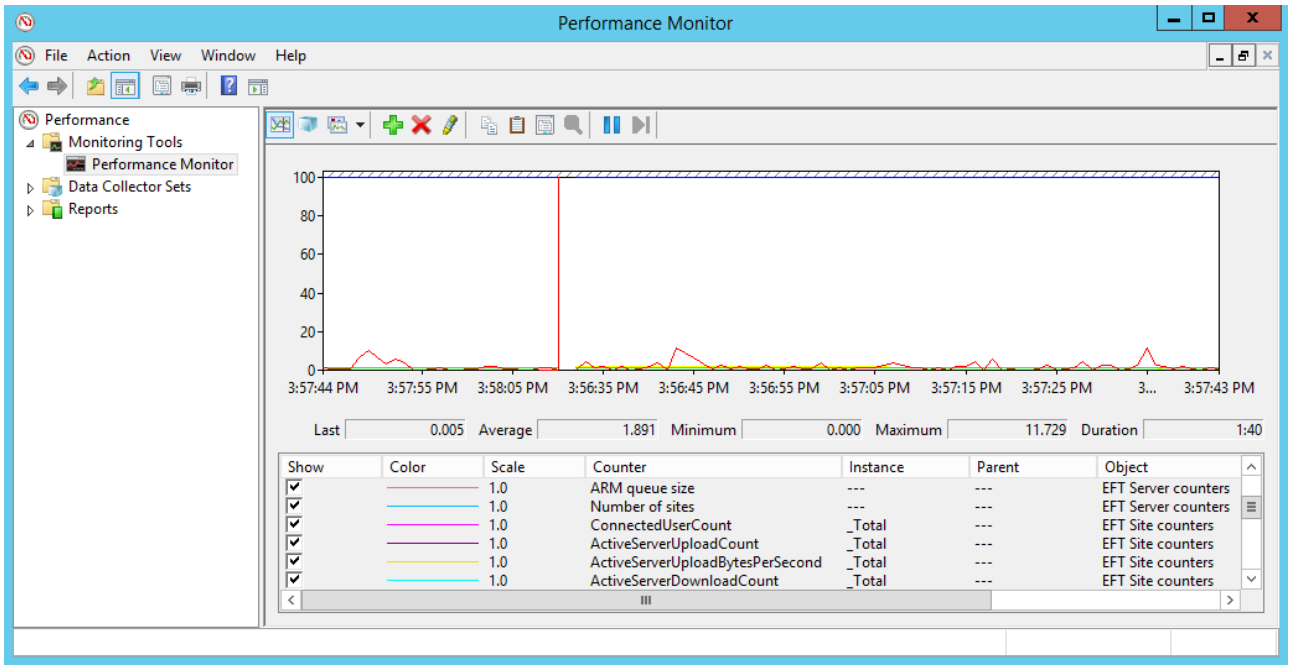
<table>
<tr><th rowspan="2">Protocol</th><th colspan="2">EFT as server</th><th colspan="2">EFT as client (that is, Event Rules)</th></tr>
<tr><th>Inbound (client push to server)</th><th>Outbound (client pull from server)</th><th>Outbound (EFT pushing to client)</th><th>Inbound (EFT pulling from client)</th></tr>
<tr><td>HTTP</td><td>%</td><td>%</td><td>%</td><td>%</td></tr>
<tr><td>HTTPS</td><td>%</td><td>%</td><td>%</td><td>%</td></tr>
<tr><td>FTP</td><td>n/a</td><td>%</td><td>%</td><td>%</td></tr>
<tr><td>FTPS</td><td>n/a</td><td>%</td><td>%</td><td>%</td></tr>
<tr><td>SFTP</td><td>n/a</td><td>n/a</td><td>%</td><td>%</td></tr>
</table></td><td>x</td><td>x</td></tr>
<tr><td>Rate</td><td>Rate, in kilobits per second (kbps), at which the file is transferred</td><td>x</td><td>x</td></tr>
<tr><td>Elapsed</td><td>Time in HH:MM:SS that it took to transfer the file</td><td>x</td><td>x</td></tr>
</table>

Performance Counters

EFT can publish a series of counters to Window's Performance Monitor (search Windows for *perfmon*). Counters are used to provide information as to how well a system is performing. This data can help administrators better understand crucial performance metrics and size the requirements of their EFT infrastructure as new requirements are placed on the system.

To view EFT counters

1. In the Windows **Search** box, type `perfmon`, and then click **Performance Monitor**.
2. In the navigation pane, expand**Monitoring Tools**, click **Performance Monitor**.
3. Click anywhere In the right pane, then click **Add Counters**.
4. In the **Add counters**dialog box, scroll through the alphabetized list to find EFT counters.
5. Click the counters, click **Add >>**, then click **OK**.
6. Clear or select the check boxes that you want to hide or show.



Below is a description of each Counter:

Server-Level Counters	Counter	Description
	Admin Accounts	Number of administrator accounts defined for this server
	Admin Accounts Locked Out	Number of administrator accounts currently and temporarily locked out of the server
	Admin Sessions	Number of authenticated administrators with an active session
	ARM Queue Size	Size of audit queue. Values exceeding ten thousand may indicate problems with your database
	ARM Stalled Audit Events	Number of audit events delayed for longer than ARMLogStalledThreadministratorDuration(The duration is set to 1 second by default.)
Number of sites	Sites	Number of Sites currently defined for this server. Updated infrequently
	Sites Enabled	Number of Sites enabled
	Sites Started	Subset of defined Sites that are actively listening for connections. Updated infrequently
WorkspacesNormalLicensesUsed	Workspaces Licenses Assigned	Total number of Workspaces in use and not expired. Includes folder shares, file sends, and drop-offs
WorkspacesLicensesAvailable	Workspaces Licenses Available	Total number of Workspaces licenses available for use or assignment

Site-Level Counters	Counter	Description
Number of running event rules	Event Rules	Number of rules defined on the Site
	Event Rules Size of Async Events Queue	Size of asynchronous event queue. Values exceeding a few score should be looked at.
ActiveClientDownloadCount	Event Rules Client Downloads	Active downloads from a remote server originating from EFT as a client
ActiveClientDownloadBytesPerSecond	Event Rules Client Download Bytes /sec	Rate at which EFT-initiated downloads are occurring measured in bytes transferred

Site-Level Counters	Counter	Description
ActiveClientUploadCount	Event Rules Client Uploads	Active uploads to a remote server originating from EFT as a client
ActiveClientUploadBytesPerSecond	Event Rules Client Upload Bytes /sec	Rate at which EFT-initiated uploads are occurring measured in bytes transferred
	Event Rules Disabled	Event rules currently disabled. You can configure a script to alert you if this number exceeds a defined threshold
	Event Rules Running Async Events	Number of running asynchronous events. A high number could indicate a need for more nodes or improved rule logic
Number of running Advanced Workflow Actions	Event Rules Running Advanced Workflow Tasks	Number of running Advanced Workflow workflows. A high number could indicate a need for more nodes or improved workflow logic
Number of running Cloud Upload Actions	Event Rules Running Cloud Upload Actions	Number of event rule actions uploading to a cloud storage provider such as Azure or AWS
Number of running Cloud Download Actions	Event Rules Running Cloud Download Actions	Number of event rule actions download from a cloud storage provider such as Azure or AWS
Number of running Download Actions	Event Rules Running Download Actions	Number of event rule actions where the action is downloading a file from a remote host
Number of running Upload Actions	Event Rules Running Upload Actions	Number of event rule actions where the action is uploading a file to a remote host
	Event Rules Size of Async Events Queue	
Size of Advanced Workflow Actions queue	Event Rules Size of Advanced Workflow Actions Queue	Size of Advanced Workflow queue. Values exceeding a few score should be looked at

Site-Level Counters	Counter	Description
	Event Rules Triggered	Number of event rules currently active. A high number could indicate a need for more nodes or improved rule logic
	Folder Monitor Worker Threads	
	Socket Connection /sec	
	Templates	Number of Templates defined for this Site. Updated infrequently. (Note that the is a "hidden" template for Remote Agents.)
	Timer Rule Worker Threads	
Number of clients	User Accounts	Number of User accounts defined for this Site. Updated infrequently.
	User Accounts Disabled	Subset of this Site's User accounts that are currently in a disabled state. Updated infrequently.
	User Accounts Locked Out	Subset of this Site's User accounts that are currently locked out. Updated infrequently.
ActiveServerDownloadCount	User Downloads	Active downloads from EFT originating from remote clients. Juxtapose with CPU, disk, network, and similar metrics to assess performance impact
ActiveServerDownloadBytesPerSecond	User Downloads Bytes /sec	Rate at which downloads are occurring by connected clients measured in bytes transferred
	User Login Failed Bad Password /sec	Rate at which user are failing to authenticate due to a valid username but invalid password being provided. There are mitigation techniques you can use if frequent attacks on root or administrator
	User Login Failed Non-existent Username /sec	Rate at which user are failing to authenticate due to an invalid or non-existent username being provided.

Site-Level Counters	Counter	Description
	User Login Success /sec	Rate at which users are authenticating successfully and turn into an active session. See User Sessions for count of actively connected users.
ConnectedUserCount	User Sessions	Number of authenticated users with an active session. Does not count stateless HTTP/S connections
ActiveServerUploadCount	User Uploads	Active uploads to EFT originating from remote clients. Juxtapose with CPU, disk, network, and similar metrics to assess performance impact
ActiveServerUploadBytesPerSecond	User Upload Bytes /sec	Rate at which uploads are occurring by connected clients measured in bytes transferred
WorkspacesDropoffLicensesUsed	Workspaces Drop-offs	Number of drop-off requests active and not expired
	Workspaces File Sends	Number of file send operations that are active and have not yet expired
	Workspaces Folders Shared	Number of folder shares that are active and have not yet expired

See also Measuring EFT Performance with Perfmon.

For information about using Performance Monitor, refer to Windows Performance Monitor Overview on the Microsoft Tech Community website.

Site Configuration

The topics below provide information regarding creating and managing Sites in the administration interface.

- How EFT Sites are Defined
- Creating a Site
- Creating a Advanced Security Site
- Propagating an EFT Site
- Starting and Stopping a Site
- Renaming a Site
- Searching a Site
- FTP/S
- HTTP/S
- SFTP
- AS2
- Connection Settings
- Automatically Creating a Home Folder for New Users
- Azure Data Lake Storage
- Banning Unwanted File Types
- Changing a Site's IP Address or Port
- Changing a Site's Root Folder
- Connection Limits Dialog Box
- Controlling Access to the Site by IP Address
- Configuring Azure Key Vault Support for EFT
- Configuring the Secrets Module
- Content Integrity Control (CIC)
- Deleting a Site
- Enable EFS Encryption
- EFT Secrets Primer (Knowledgebase)
- Enabling the Account-Management Page
- Enable and Configure EFT Workspaces
- Encrypted Folders (EFT Encrypted)
- Encryption Algorithms

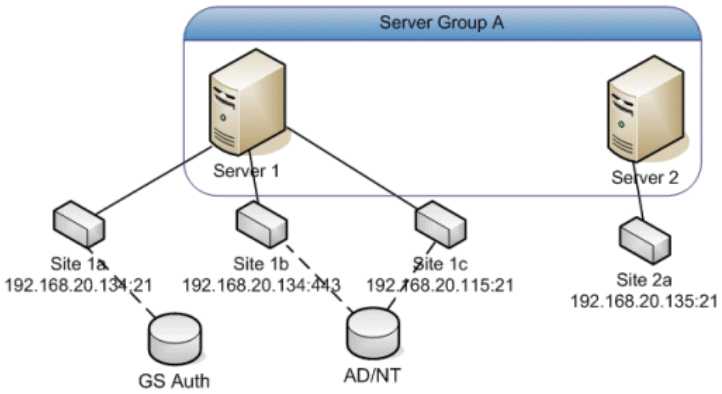
- Flooding and Denial of Service Prevention
- Internal Domain Settings
- Override VFS Credentials
- Proxy Protocol
- Runtime Template Variables
- Setting Maximum Concurrent Socket Connections
- Setting Maximum Concurrent Logins
- Setting Maximum Connections per User
- Setting Maximum Connections per IP Address
- Setting Maximum Transfers per Session
- Setting Maximum Transfer Size
- Setting Maximum Transfer Speeds
- Specifying External and Internal Domains
- Specifying File Deletion Options
- Unicode Exceptions
- Unicode File Transfers
- User Account Details Template
- User Database Refresh
- Viewing Site Statistics
- Viewing Connections to a Site
- Viewing Transfers To and From the Site

How EFT Sites are Defined

In EFT hierarchy, *Server Groups*are at the top of EFT's setting hierarchy and allow you to group multiple Servers from a management or administrative perspective. A *Server* consists of one or more physical hardware devices or virtual servers running the EFT executable as a system service. Each EFT service can support multiple *Sites*. A *Site* in EFT is similar to a virtual FTP server bound to one or more IP addresses.

You cannot run multiple Sites on the same IP address and port. Each Site requires an IP address and port combination that is not already claimed by other process or Site. To avoid conflicts, when the same protocol is used, each Site requires a distinct IP address (and same port), or the same IP address, but different ports. For example, use port 8080 for HTTP instead of 80, or 2121 for FTP instead of 21. You cannot have two Sites trying to use port 21 on the same IP address. The two Sites will conflict; the Site that starts first claims the contested port.

The hardware in EFT's computer does not limit the number of Sites you can set up, at least regarding how many NICs (Network Interface Cards) you have. In Windows, you can assign any number of IP addresses to a single NIC.



In the above example, your internal users could connect to site 1A using the Site's internal IP address (192.168.20.134:21) while external users can access site 1C using the host address you designate, such as *partners.globalscape.com*, which resolves to a different IP address on the same port).

Sites can each have a unique authentication provider type, the same authentication provider type, or even share the same authentication provider database. For example, Site 1A could use Globalscape Authentication, Site 1B could use Active Directory (AD), and Site 1C could share the AD database.

The EFT service runs under a user account, which must have full administrative rights to the folder in which you installed EFT. With administrative rights, the EFT service can save all your settings. If the EFT service does not have administrative rights, you lose

settings and user accounts whenever you restart the EFT service, and you need to reset permissions on the computer where the EFT service is running.

You will need the following information to create and configure a Site:

- Site name, listening IP address, and administrator port
- Root folder path
- DMZ Gateway IP address and port, if used
- SSL/SFTP keys/certificate/ciphers/version information

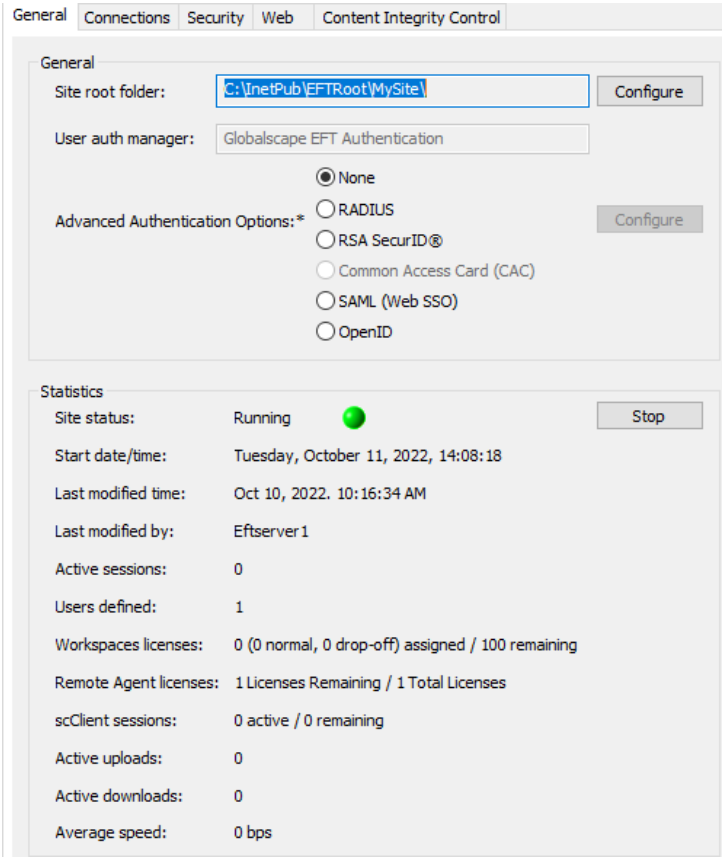
Site SettingsTabs

When you click a Site node on the **Server**tab, tabs appear in the right pane in which you can configure connections to the Sites.

- General Tab of a Site
- Connections Tab of a Site
- Security Tab of a Site
- Content Integrity Control Tab
- Web Tab

General Tab of a Site

The **General** tab is used to change the Site's user authentication settings, view Site statistics, and stop/start the Site.



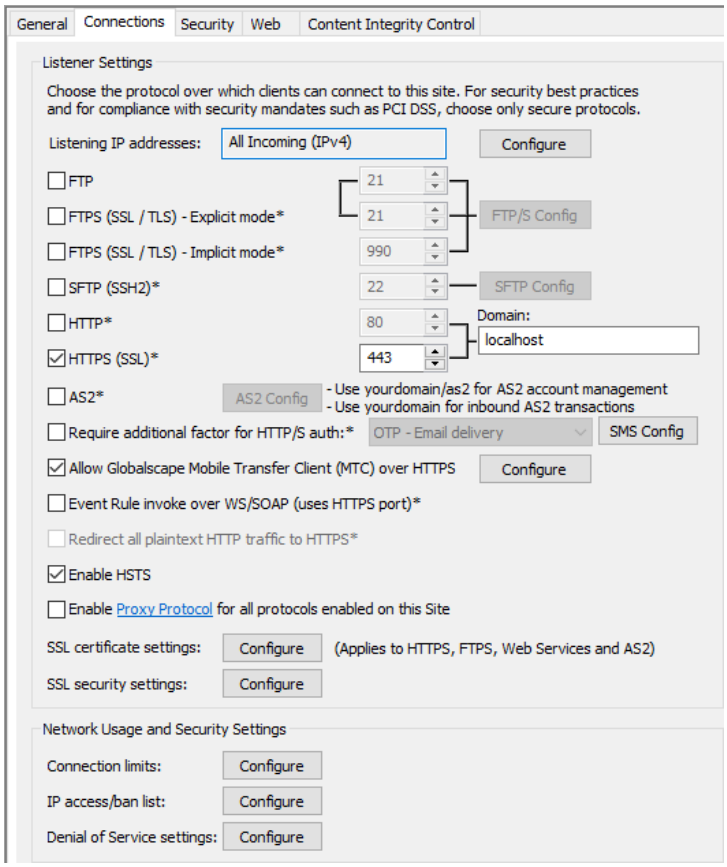
Related Topics

- Changing a Site's Root Folder
- Configuring Windows NT Authentication Options
- Changing and Testing LDAP Authentication Options
- Configuring ODBC Authentication Options
- Configuring RSA SecurID or RADIUS Support on an Existing Site
- RADIUS for User Authentication
- CAC for User Authentication
- SAML (Web SSO) Authentication
- OpenID Configuration
- Starting and Stopping a Site

- Viewing Site Statistics
- Workspaces Licenses

Connections Tab of a Site

The **Connections** tab of a Site is used to specify listener settings, transport protocols, the SSL certificate for the Site, connection limits, the IP address access/ban list, Denial of Service (DoS) settings, and for enabling web features.



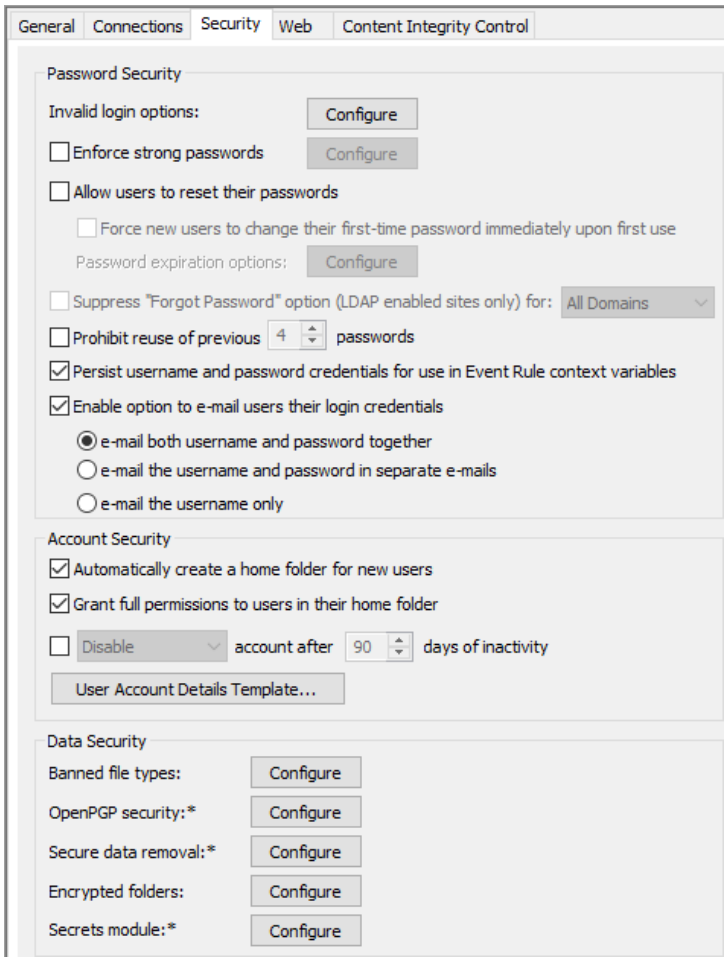
Related Topics

- Listener Settings **(including information about the Domain box)**
- Connection Limits Dialog Box
- Controlling Access to the Site by IP Address
- Flooding and Denial of Service Prevention
- Configuring FTP Transfers on the Site
- Site-Level Blocking and Timeout Settings
- Modifying Site Messages
- Multi-Part Transfers
- Enable Multifactor Authentication for Workspaces
- SFTP

- SSL
- Configuring HTTP or HTTPS Transfers on the Site
- Redirecting HTTP to HTTPS
- Enable HSTS
- Proxy Protocol
- Configuring the AS2 Module
- Connection Limits Dialog Box
- Controlling Access to the Site by IP Address
- Flooding and Denial of Service Prevention
- Enabling the Mobile Transfer Client
- Enabling and Using Web Services (WS/SOAP) in Event Rules
- Enabling User Access to the Web Transfer Client

Security Tab of a Site

The **Security** tab of the Site node is used to specify password security, account security, and data security settings.



Related Topics

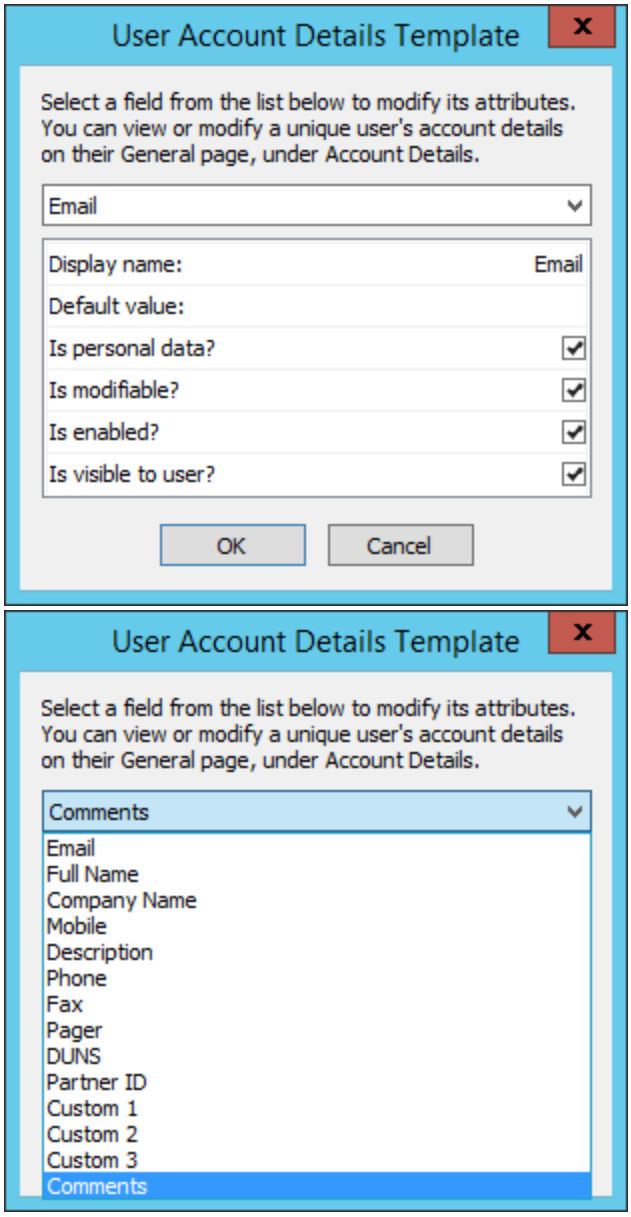
- Disabling or Locking out an Account after Invalid Password Use
- Banning an IP Address that Uses an Invalid Account
- Configuring the Secrets Module (Using the Azure Key Vault)
- Emailing Users' Login Credentials
- Automatically Creating a Home Folder for New Users
- Deleting or Disabling Inactive User Accounts
- Banning Unwanted File Types
- Setting OpenPGP Security for the Site
- Specifying File Deletion Options

- Encrypted Folders
- Using Login Credentials in Event Rules
- Suppress "Forgot Password Option"
- User Account Details Template

User Account Details Template

The **User Account Details Template**, available from the **Site > Security**tab, allows you to define which privacy rules will apply to the user account details for ***all***user accounts on the Site. Designating attributes to existing account detail fields helps you manage user account details and privacy settings for the purposes of privacy regulations, such as GDPR.

(Changes to the template only affect new users; existing users' settings will not be changed unless you reset the fields on the **User Account Details** dialog box for each of those users, as described below.)

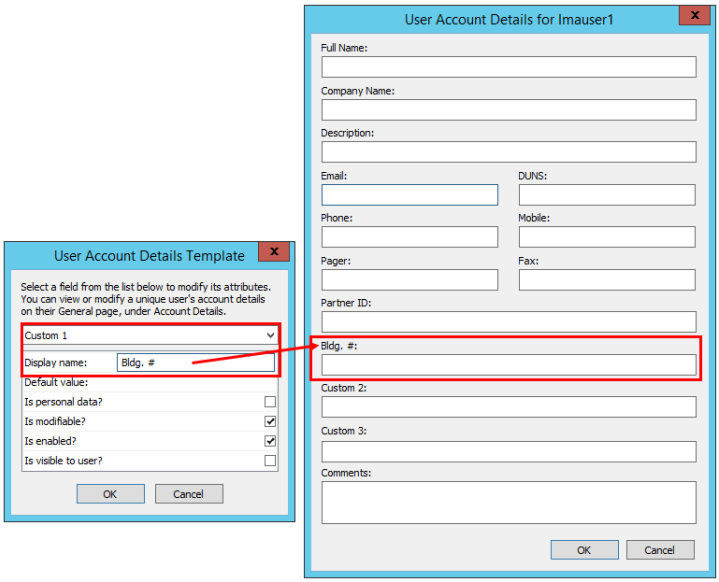


To change the user account fields attributes, default value, and display name

1. For each User Account Details field, select it in the drop-down list, then select or clear the attribute check box for each field:
   - **Is personal data:**Specifies whether this field is considered personal data as classified by GDPR or other privacy laws
   - **Is modifiable:** Specifies whether this field's value can be modified (by an administrator or, if applicable, by the user)
   - **Is enabled:** Specifies whether the field is enabled. If set to false, the field's value will remain intact, but the data will be inaccessible to EFT for use (for example, in event rules)
   - **Is visible:** Specifies whether the field's value is visible in the Web Transfer Client (if you change the **Display Name**of the field, the new name is not displayed in the WTC)
2. When you specify a **Default value** (optional), you are then asked if you want this new default value to apply to **Existing & New** users or **Just New**users.

   - When using external authentication databases, user account details must be changed on the authentication database.
   - Those settings should be visible in the Web Transfer Client, but not editable. For example, EFT is unable to write changes to a LDAP server, therefore, for those fields, such as email address, you should clear the **Is modifiable**check box.
   - On AD-authenticated Sites, the EFT administrator can edit the **User Account Details**field names, but they will be overwritten when the AD user database is refreshed.
   - Account details fields are not modifiable in the WTC for EFT users on an AD site.
   - Account details fields are modifiable in the WTC for Guest users on an AD site.

3. The **Display name** can be edited, and the change will appear in the**User Account Details** dialog box. However, the field name in the database will remain the same. For example, you could change Custom 1 to display the building number in which a user works. It will display the new field name in the **User Account Details** dialog box, but not in reports or the WTC.



The user account logon name appears in the Title bar of the **User Account Details** dialog box. Even when the EFT administrator does not have **Manage Personal Data** enabled, the logon name for the user account will appear in the Title bar, Settings Template tree, and in logs. For additional user privacy, the EFT administrator and users can specify safer login attributes. For example, by default, an LDAP Site uses the "cn" attribute for the account name. Instead, when creating an LDAP Site, the administrator can use "sAMAccountName" as the login attribute, to avoid compromising client full names.

To edit the display name

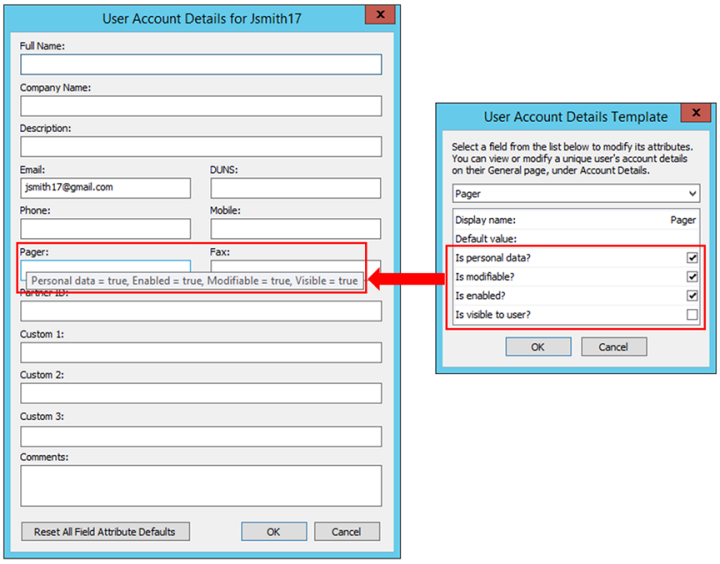
1. On the **Site > Security**tab of the account, click **User Account Details Template**.
2. Click the attribute display name and double-click the value.
3. Modify the text, then click **OK**in the **User Account Details Template**dialog box.
4. Click **Apply**.

The default setting (true or false) for each field are shown in the table below:

FieldName	Email	Full Name	Company Name	Mobile	Description	Phone	Fax	Pager	DUNS	Partner ID	Custom1	Custom2	Custom3	Comments
Display name	Email	Full Name	Company Name	Mobile	Description	Phone	Fax	Pager	DUNS	Partner ID	Custom1	Custom2	Custom3	Comments
Is Personal data?	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Is Modifiable?	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Is Enabled?	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Is Visible (to user)?	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
ContextVar	Email	FullName	CompanyName	Mobile	Desc	Phone	Fax	Pager	DUNS	PartnerID	Custom1	Custom2	Custom3	Comments

The **User Account Details Template** is the "master" for each field's attributes. If you change an attribute in the **User Account Details Template** (that is, clear or select a check box), a button appears on the **User Account Details**dialog box to indicate that the field attribute (true/false) in the user details no longer matches the template.

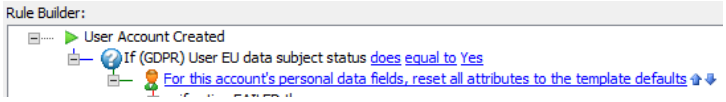
In the example below, the **Pager**field attribute in the User Account Details dialog box is "Visible = true" but the **User Account Details Template** was changed to false (cleared check box). You can leave the setting as-is in the **User Account Details** dialog box, or you can click **Reset All Field Attribute Defaults** to make the field attributes in the **User Account Details** dialog box match the template's settings.



To make attribute changes to specific accounts

1. Create an Event Rule using the **User Account Created** event.
2. Add the **If (GDPR) User EU data subject status** Condition to the Rule, and set it to **does equal to Yes**.
    - The user's EU data subject status is specified on the user account's **General** tab.
3. Add the **User Account Action**to the Rule, and select the option **For this account's personal data fields, reset all attributes to the template defaults**.

This Event Rule will set the attributes of all personal data fields to the template defaults each time a new user account is created.



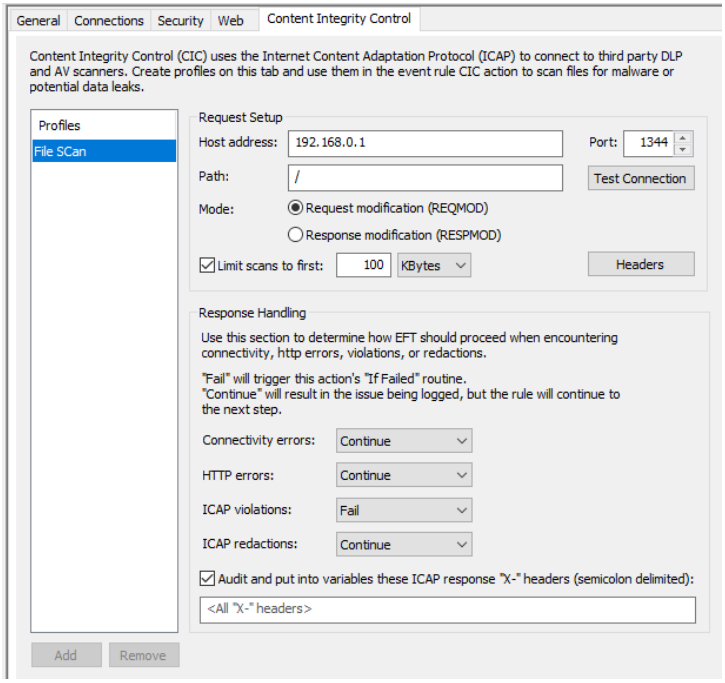
Related Topics

- Creating a User Account
- Configuring User Account Details
- Privacy Policy
- Specify Terms of Service and Privacy Policy Options

Content Integrity Control Tab

Content Integrity Control is used to send a file to an antivirus scanner or data loss prevention solution for processing. When a **File Scan** Action is added, a file that triggers the Event Rule is sent to an ICAP server for processing. When the file passes, other Actions can occur, such as moving the file to another location. If the file fails, processing can stop, or other Actions can occur, such as sending an email notification.

Refer to Global Antivirus Scanning for details of configuring Global antivirus on this tab.



To remove a profile

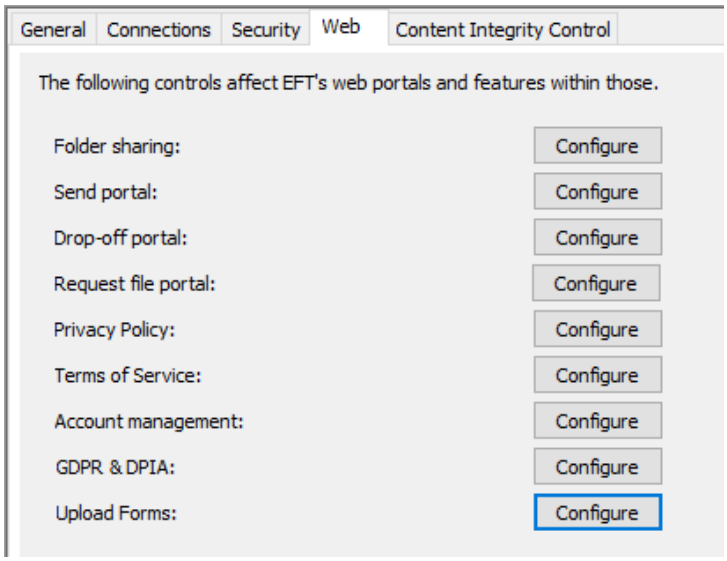
- To remove a profile, select its name in the list, and then click **Remove**.

Related Topics

- Global Antivirus Scanning
- File: Scan Action (CIC)
- EFT Specifications

Web Tab

On the Site's **Web** tab, you can configure web portal controls and features. (This tab replaces Workspaces tabs and other web-related features from previous EFT versions.)



Related Topics

- Folder sharing - Enable folder sharing, Workspaces configuration, and Guest Account controls
- Send portal - Enable and configure the EFT Outlook Add-In and enable Reply Portal
- Drop-off portal - Enable anonymous drop-off portal, enable and configure CAPTCHA, specify message size, domains, and "To" aliases
- Request file portal- Enable non-guest account owners to request files from others
- Privacy Policy - Enable and configure Privacy Policy
- Terms of Service - Enable and configure Terms of Service
- Account management - Enable the account management page
- GDPR & DPIA - Configure GDPR settings
- Upload Forms - Create and edit upload forms

Creating a Site

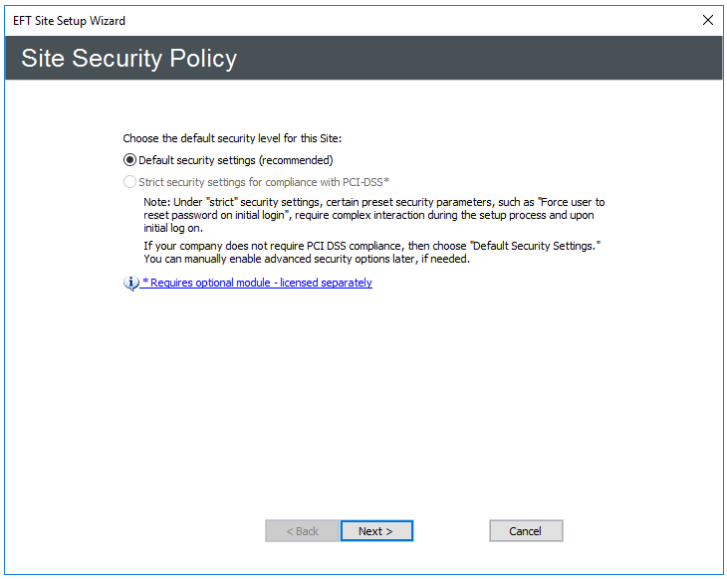
A *Site* is how you connect to EFT. This topic describes how to create the connection, including IP address, port, and so on.

> **NOTE:** Configuring an EFT site with a long path is not supported. (TFS389235)

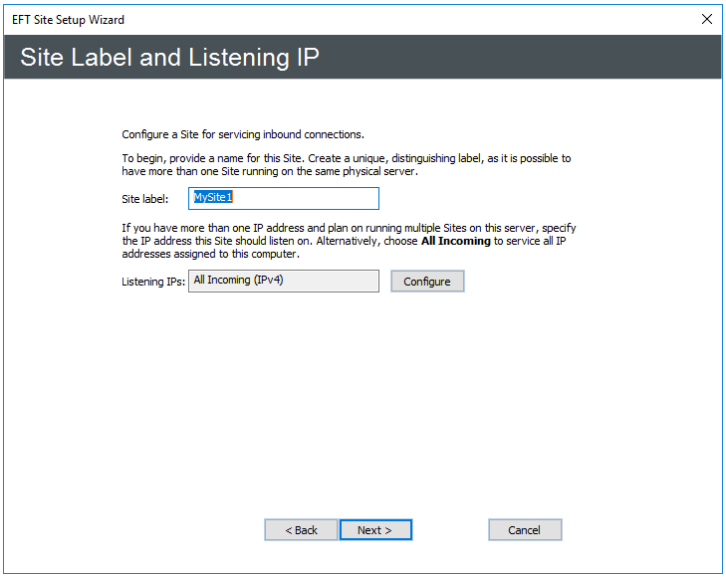
To create a Site

1. The **Site Setup**wizard appears automatically after you complete the **Server Setup** wizard; otherwise, do one of the following:
    - In the administration interface, click **Configuration >Create New Site**.
    - Right-click anywhere in EFT's tree, then click **Create New Site**.

      The **EFT Site Setup Wizard** appears.



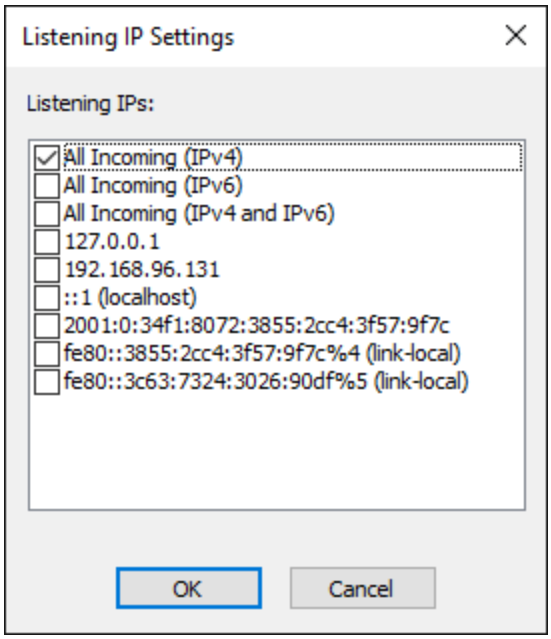
2. You are asked to choose the **default security level** for the Site. If PCI DSS compliance is not a requirement, you can use the default security settings and then manually configure advanced security options individually, as needed. Do one of the following:
    - To create a Site that complies with PCI DSS, refer to Creating a strict security-enabled Site.
    - To create a standard Site, click **Default security settings**.
3. Click **Next**. The **Site Label and Listening IP**page appears.



4. In the **Site label**box, type a distinguishing name for the Site. `MySite`appears by default, but you can change this to anything you want.

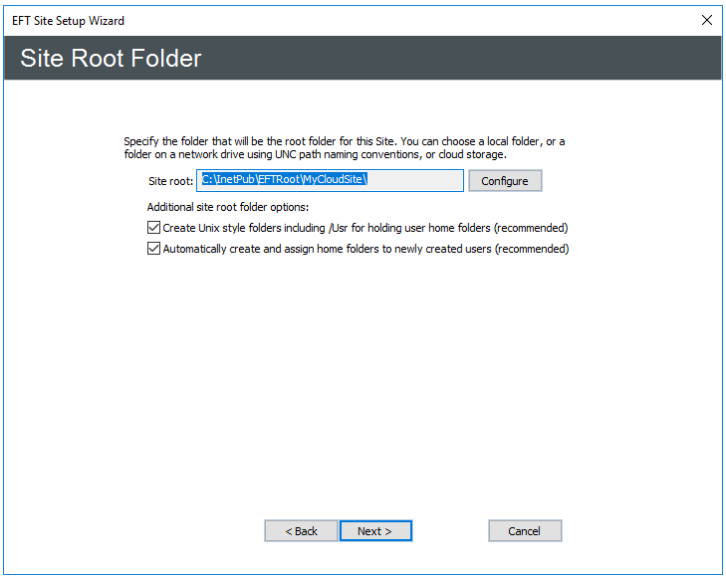
    The Site name cannot have a period at the end of the name or use any characters that are not allowed in Windows file naming. The Site label is also used in the Virtual File System (for example, **C:\Inetpub\EFTRoot\MySite\Usr**) and in logs and reports.

5. Next to the **Listening IPs** box, click **Configure**. The **Listening IP Settings**dialog box appears.

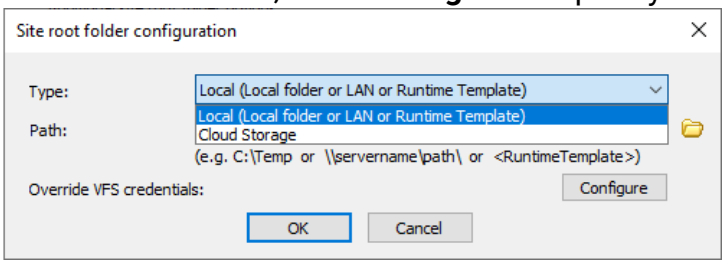


- The dialog box displays the IP addresses that are available on the computer, in addition to **All Incoming (IPv4)** and **All Incoming (IPv6)**.
- You cannot type in an address.
- IPv6 is not enabled by default for security reasons; IPv4 is enabled by default.
- The "All" options are exclusive. That is, you can't select **All Incoming (IPv4)** and then one or more specific IP addresses. However, you can select multiple individual addresses if none of the "All" options are selected.
- "Link local" appears next to certain IPv6 addresses. Routers do not forward packets with link-local addresses. In IPv6, link-local addresses are always assigned, automatically or by configuration, and are required for the internal functioning of various protocol components. IPv6 requires operating systems to assign link-local addresses to network interfaces even when routable addresses are also assigned. A link-local Unicast address has the prefix fe80::/10 in standard IPv6 CIDR notation.

6. Select one or more check boxes for the IP addresses on which the Site is to listen for connections, and then click **OK**. The selected addresses appear in the **Listening IPs** box.
    - You can copy the addresses in the **Listening IPs** box: Right-click in the box, click **Select All**, then right-click again and click **Copy**or use CTRL+V. (Unicode-related items on the right-click menu are a Windows feature and do not apply to EFT.)
7. Click **Next**. The **Site Root Folder** page appears.

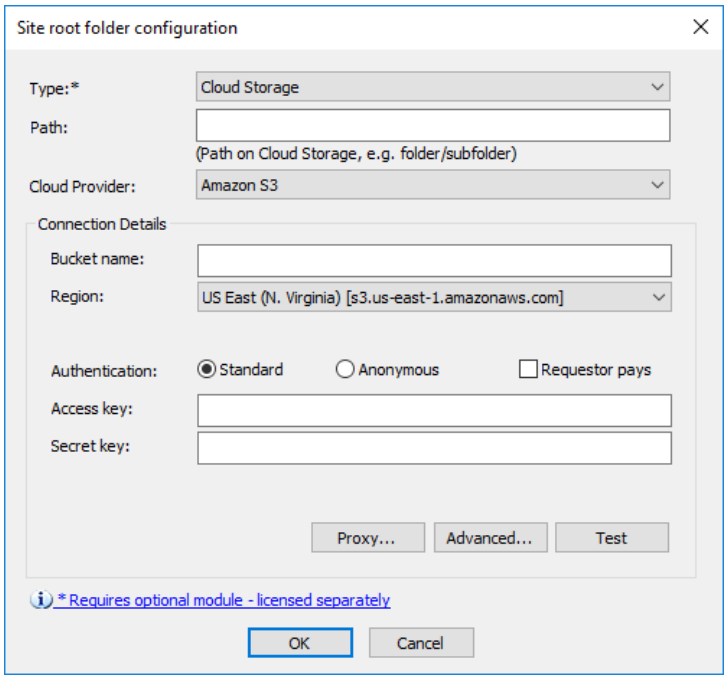


8. In the **Site root**box, click **Configure** to specify the root folder.



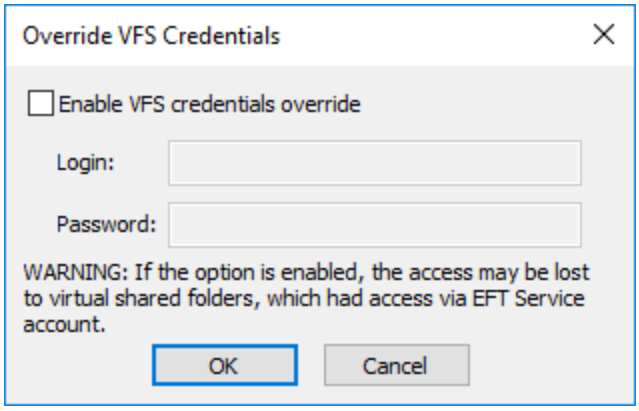
- In the **Type** drop-down list, click **Local** or **Cloud Storage**.
- In the **Path** box, provide the path to the Site root folder, or keep the default displayed in the **Path** box.
  - If you choose **Local**, provide the path to the local folder or keep the default. If you type a folder path that does not exist, it will be created.
  - If you choose **Cloud Storage**, the cloud storage location must exist; EFT will not create it.

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.



- Refer to Changing a Site's Root Folder for details of configuring cloud storage as the Site's root.

- To enable VFS credentials override, click **Configure**.



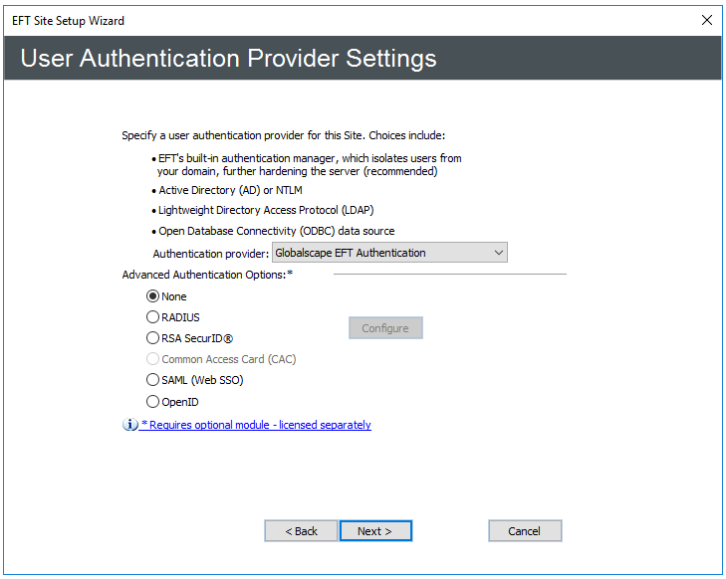
- Select the **Enable** check box, the provide the **Login** and **Password**.

9. In the **Additional site root folder options**area, select the check boxes as needed:
   - Select the **Automatically create UNIX-style subfolders** check box to create **Usr**, **Pub**, **Bin**, and **Incoming**folders with appropriate permissions under the Site's root folder. This is only necessary if you are trying to mimic a typical default *nix EFT setup. It is selected by default.
   - Select the **Automatically create and assign home folders to newly created users** check box to automatically create a user folder under **\Site Root\Usr** when a new user is added. The folder name is the same as the

username. For example, username `jbite`would have the folder **C:\InetPub\EFTRoot\MySite\Usr\jbite**.

On an AD-authenticated Site, if **Automatically create and assign home folders to newly created users** is enabled, EFT creates a virtual folder under the Site's physical root that points to the user's home folders assigned in AD. If **Automatically create and assign home folders to newly created users** is disabled, the functions for creating virtual or physical folders for AD users are disabled.

10. Click **Next**. The **User Authentication Provider**page appears.



11. Under **Advanced Authentication Options**, configure one of the following options (Requires AAMM):
    - **None** - If you are not using RADIUS, RSA, or Common Access Card (CAC), or SAML (WebSSO)
    - **RADIUS**- If EFT is connecting to a server using RADIUS, click **Configure**. and configure the site to use RADIUS for authentication.
    - **RSA SecurID**- If EFT is connecting to a server using RADIUS, click **Configure** to configure the Site to use RSA SecurID.
    - **Common Access Card (CAC)** - If this Site is using CAC authentication, no further configuration of EFT is required. (Available only on LDAP Sites)
    - **SAML (Web SSO)**- If this Site is using **SAML (WebSSO)**, click **Configure** and provide the details needed to configure SAML, then click **OK**.
    - **OpenID** - If this site is using OpenID for authentication, click **Configure**, provide the details needed to configure OpenID, then click **OK.**

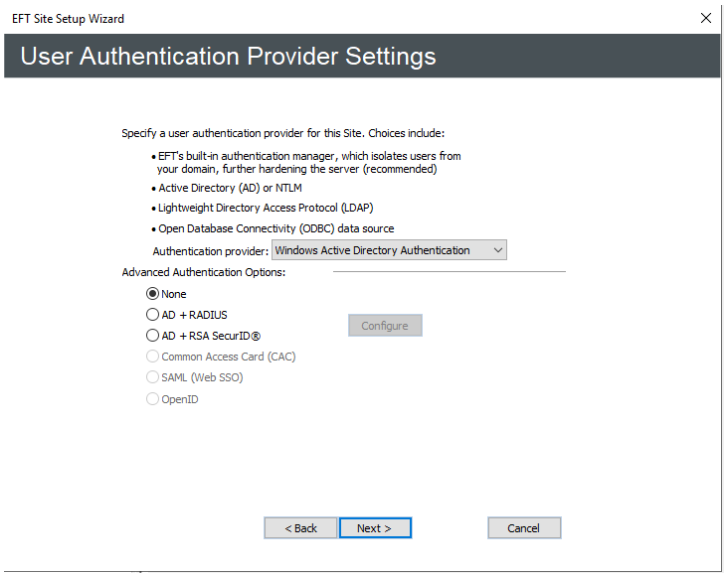
12. In the **Authentication provider**list, specify the type of user authentication this Site is to use. (Click a link below to skip to that section.)
    - Globalscape EFT Authentication- Does not rely on outside sources for user information. All information in the authentication database is protected from the operating system, contained within EFT, and can only be modified through the administration interface.
    - Windows Active Directory (AD) Authentication- Connects to an AD server for user information.
    - LDAP Authentication - Connects to an LDAP server for user information.
    - ODBC Authentication - Connects to an ODBC database for user information.

    For Globalscape EFT Authentication

    a. Verify that **Globalscape EFT Authentication**is specified, and then The **EFT Server Authentication** page appears.
    b. The default path to store the user database appears in the box. If you want to store the user database in a different location, type the path in the box or click the folder icon to find and select or create a folder.
    c. Click **Next**. The Perimeter Network Security page appears.

    For Windows Active Directory Authentication

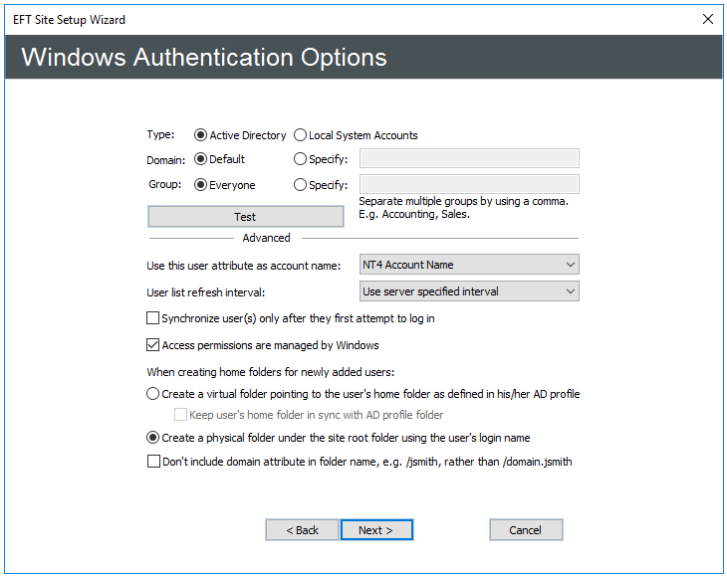
    a. EFT is installed by default under the "local system" account, which cannot log in to AD. EFT must be running under an account that has permission to access the domain controller (that is, create a domain account for EFT). Each Site can connect to only one domain. To connect to multiple domains, you must create multiple AD Sites.
    b. In the **Authentication type** list, click **Windows Active Directory Authentication**.



c. Under **Advanced Authentication Options**, leave the default of **None**, or specify whether you are using **AD + RADIUS**, or **AD + RSA SecurID®**. (These options are unavailable if you have not licensed the Advanced Authentication module.)

d. Click **Next**. A prompt reminds you that you need to specify a "Log on as" user account for EFT instead of "Local System."

e. Click **OK**. The **Windows Authentication Options**page appears.



f. In the **Type**area, click **Active Directory**or **NTLM/Local System Accounts**to match the authentication method used on EFT's domain. Authentication is done with Microsoft's LogonUser() function in Windows. The operating system then determines which method to use for authentication, such as

Kerberos, NTLM2, etc.

- **Active Directory**- EFT queries the domain controller for the list of users and groups.
- **NTLM Authentication/Local System Accounts** - EFT queries the local system to get the list of users and groups.

  If EFT is installed in HA mode, you cannot use Local System Accounts.

g. In the **Domain**area, do one of the following:
   - Click **Default**if you want to use the authentication database on the computer's current domain.
   - Click **Specify**, then in the box, provide the domain name that contains the authentication database.

h. In the **Group**area, do one of the following:
   - To allow access to every user in the domain's database, click **Everyone**.
   - To allow access to only a specific AD Group, click **Specify**, then in the box, type the AD group name for users that will have access to EFT.

   For information about support for foreign groups, refer to Support for Foreign Groups.

h. To verify your settings, click **Test**.

i. To close the **Test** dialog box, press ESC.

j. In the **Use this user attribute as the logon name** box, click the list to specify the attribute to use (only available when AD authentication is selected):
   - **NT 4 Account Name** - Username
   - **Display Name**- (DN) When a new user is created in Active Directory, the Full name field is always generated in FirstName LastName format. This field sets the Display Name field on creation, and you end up with a FirstName LastName formatted global address list.
   - **User Principal Name** - (UPN) For example, your_user_name@mycompany.com
   - **Common Name**- (CN) fully qualified domain name, computer name (netbios), localhost

Regardless of the logon name chosen, EFT will accept the provided logon name type, whether UPN, NT4 account name, common name, or display name, and if a match exists, the user will be authenticated and the chosen logon name type will be displayed in the administration interface.

Logon name type	Allowed login form
NT4 Account Name (NT4)	NT4/UPN
Display Name (DN)	DN/NT4/UPN
User Principal Name (UPN)	UPN/NT4
Common Name (CN)	CN/NT4/UPN

k. In the **User list refresh interval** box, click the list to select how often you want EFT to check the authentication database for new users (server specified, never, or from 5 minutes to 1 day).

l. To use AD to authenticate users both in the portal and in the Outlook Add-In using EFT permissions for folder access, select the **Access permissions are managed by Windows**check box. This property is read-only after the Site is created.

   If this check box is ***NOT***selected (disabled/turned off):

   - The VFSsubtree in EFT is manageable and works similarly to non-AD-authenticated Sites.
   - The **Groups**node works similarly to non-AD-authenticated Sites.
   - When the user account log in to the Site (via HTTP/FTP/etc.), EFT uses the credentials (username+password or IWA) to authenticate the client against AD/NTLM, then discards the impersonation token, and all further file/folder operations are done on behalf of EFT's system account, similarly to non-AD-authenticated Sites.
   - Access permission is defined by EFT in VFS.
   - **Create a virtual folder** and **Keep user's home folder** check boxes appear dimmed in the Site wizard and the Site General tab. These measures prevent clients from getting their EFT home folder mapped to their AD home folder, which most likely does not have access permissions for EFT's system account.
   - EFT does not show the standard "The service may not have adequate permissions depending on your AD configurations" prompt when the administrator starts editing Site authentication manager settings.
   - The authentication manager property is exposed via COM (ICIADAuthManagerSettings interface):

```
HRESULT UseWindowsAccessPermissions([out, retval]
VARIANT_BOOL* pVal); HRESULT
UseWindowsAccessPermissions([in] VARIANT_BOOL
newVal);
```

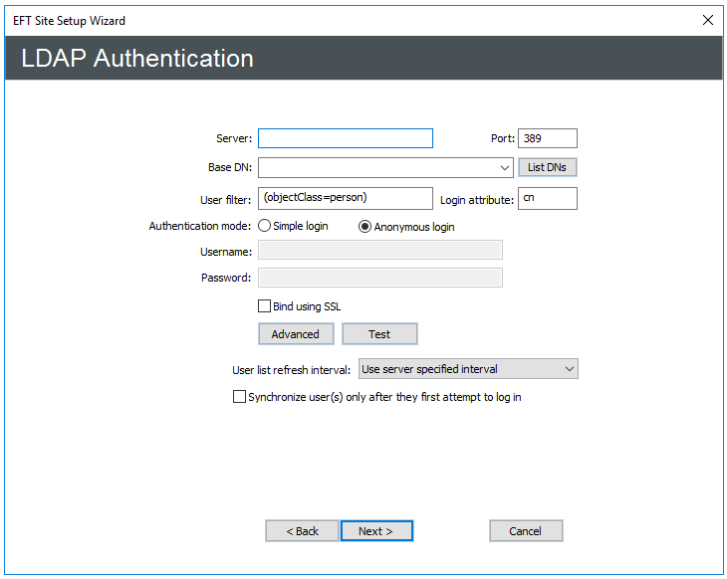
m. Under **When creating home folders for newly created users**, do one of the following:
   - If you click **Create a physical folder**, and if NT4 Account Name was selected as logon attribute, you can choose to not include the domain in the folder name by selecting the **Don't include domain attribute in folder name, e.g., /jsmith, rather than /domain.jsmith** check box.
   - If you click **Create a virtual folder**, the virtual folder will point to the user's home folder as defined in his/her AD profile. (This option is disabled if Automatically create and assign home folders to newly created usersis disabled.)
   - To keep the users' home folders updated based on the AD profile folder for the user, select the **Keep user's home folder in sync with AD profile folder** check box. Selecting this check box allows AD users that are configured with a home folder in AD to successfully create and share a Workspace.

n. **Skip to configuring** Perimeter Network Security.

For LDAP Authentication

a. If you are using Common Access Card (CAC) authentication, click **Common Access Card (CAC) authentication**. (The **Configure**button applies only to RADIUS and RSA.)

b. In the **Authentication type** list, click **LDAP Authentication**, then click **Next**. The **LDAP Authentication**page appears.



c. In the **Server**box, type the **Server** name or IP address.

d. In the **Port**box, keep the default port 389 or specify a different port used by your LDAP server.

e. In the **Base DN**box, type the base domain name for the LDAP user database, in the format `option=value`(e.g.: `dc=forest,dc=tree,dc=branch`), or click **List DNs** to complete the box automatically or select from a list.

f. In the **User Filter**box, type the search filter information. Refer to Advanced LDAP Filtering for a detailed explanation of LDAP filtering.

g. In the **Login Attribute** box, type a comma-separated list of attributes to retrieve. Add `userprincipalname`to the LDAP query so that the `userprincipalname`is used for the account name in queries. For example, type:

   `userprincipalname,mail,email,name,cn`

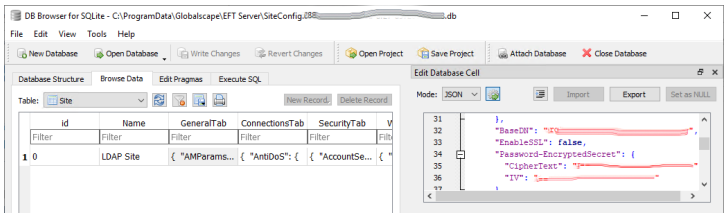
h. In the **Authentication mode** area, click one of the following binding methods to define how the client is authenticated:

   - **Anonymous**
   - **Simple**requires a username and password. If Active Directory is acting as the LDAP provider, then providing credentials the DOMAIN\username style is sufficient. The credentials provided are typically those of the service account, and the user does not need to have any elevated privileges on the AD domain, only a Domain User. Otherwise, the username must follow the syntax for the LDAP server that includes the Common Name and the Domain Components of your LDAP server's distinguished name. For example, the username

might be the following:

```
cn=Manager,dc=forest,dc=tree,dc=branch
```

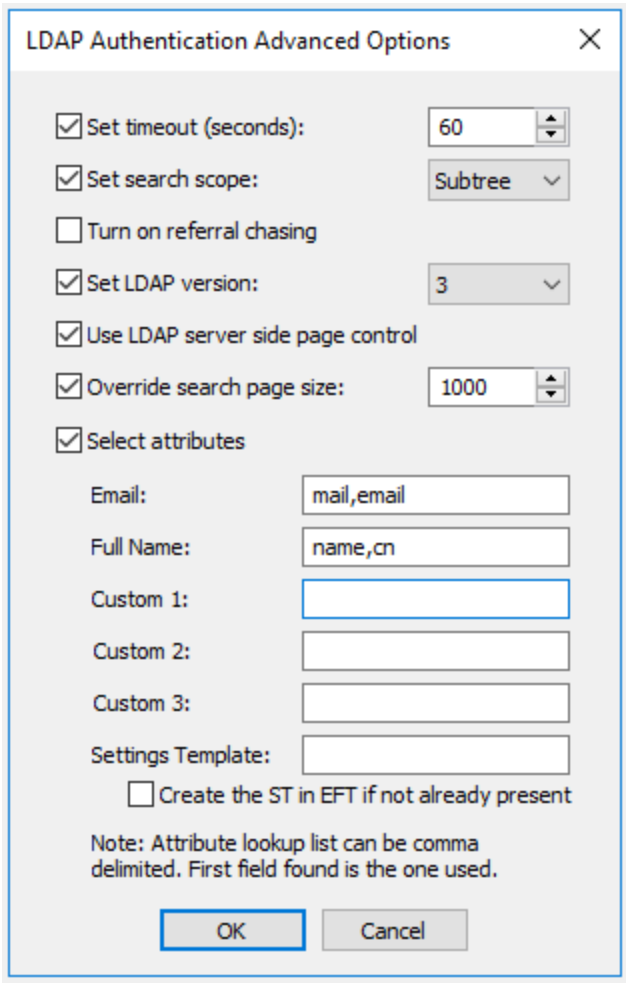
The LDAP bind password is encrypted and stored in the SQLite file, **..\ProgramData\Globalscape\EFT Server\SiteConfig.*nnnnnnnnn*.db**



i. If you want to encrypt LDAP communications, select the **Bind Using SSL** check box.

   If Microsoft's Active Directory is the LDAP provider, Certificate Services must be enabled on the domain before domain controllers will be able to receive encrypted LDAP connections.

j. Click **Advanced**. The **LDAP Authentication Advanced Options** dialog box appears.



k. Specify advanced options based on your requirements:

- **Set timeout**- Specify the connection/query timeout (in seconds). This option coupled with paging can help you avoid timeouts when querying against large directories.
- **Set search scope** - This specifies the depth of the level to search for under **BaseDN**.
  - **BASE**- Only the requested object specified in **BaseDN**is searched.
  - **OneLevel**- All of the objects just below this object are searched.
  - **Subtree -** Searches for all the objects within the specified **BaseDN** object recursively.
- **Turn on referral chasing** - If you have referral chasing on, the query returns information for objects that exist in the LDAP structure, but do not actually exist on EFT to which you are connected. The query displays bookmarks to entries that exist elsewhere in the network that EFT knows about.

- **Set LDAP Version** - LDAP 2 is widely supported and adds anonymous binding and some filtering. LDAP 3 extends the features of LDAP 2 by adding paging (server side) and more complex filtering.
- **Use LDAP server-side page control** - Asks EFT to limit result sets (or pages) to 1000 at a time or the value specified under **Override search page size**, if checked. If **Use server page control** is not selected, client-side paging is used to mitigate timeouts when retrieving large directory listings.

  If you are connecting to a SUN Directory LDAP server, turn off page control.

- **Override search page size** - Overrides the default page size (1000) for client or server-side page limits. Making the value too large can cause timeouts. Setting the page size too small reduces the overall efficiency.
- **Select attributes**- Select the **Select attributes**check box, then specify the LDAP attributes that you want to use, such as cn (common name), streetAddress, mail (email address), employeeID, employeeType, etc.
  - Multiple attributes can be added to each custom field, but only the first attribute found will be used; All other attributes will be ignored.
  - An attribute field on the LDAP server can contain multiple attributes if you want multiple attributes added to a single custom field, such as for the address.
  - Refer to Map LDAP Account Attributes to EFT User Account Detailsfor more information about LDAP account attributes.

l. Click **OK**to close the **LDAP Authentication Advanced Options** dialog box.

m. To test your settings, click **Test**. The **Authentication Manager Test Results** appear. For details of the LDAP test, refer to Testing LDAP Authentication Settings.

n. Click the **X**in the upper right corner to close the dialog box.

o. Specify the path at which EFT will store additional user settings, if different from the default shown in the wizard.

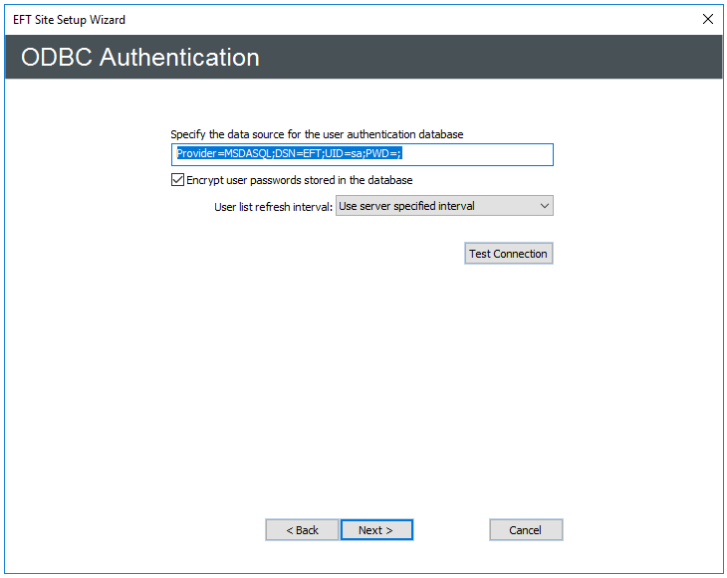
p. In the **User list refresh interval** box, specify the frequency at which EFT's user list should be refreshed. By default, the Server is configured to not refresh automatically.

This setting is disabled on HA nodes; the user list must be synchronized on all nodes at the same time.

q. **Skip to configuring** Perimeter Network Security.

For ODBC Authentication

a. Click **Next**. The **ODBC Authentication**page appears.



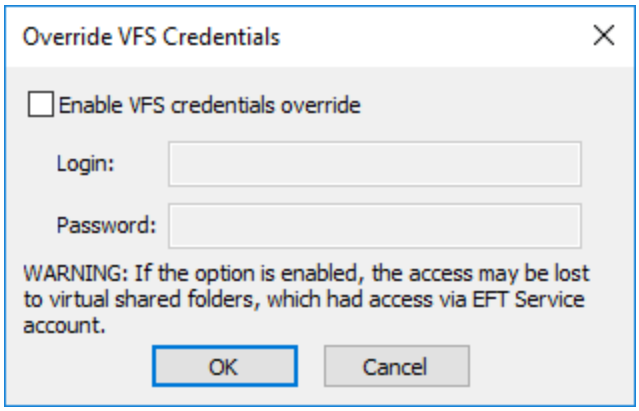
b. In the **Specify the data source** box, type a connection string for the ODBC database. Refer to Using a DSN-Less Connection with ODBC Authentication for details of creating the connection string, if necessary.

c. Select the **Encrypt user passwords** check box to encrypt passwords stored in the database. When this check box is selected, when you create user accounts within EFT, the ODBC database is populated with the username and a SHA-256 hash of the account password. Alternatively, you can set a value in the registry to use MD5 encrypted passwords instead.

d. In the **User list refresh interval** list, click the list to specify how often you want EFT to check the database for new users.

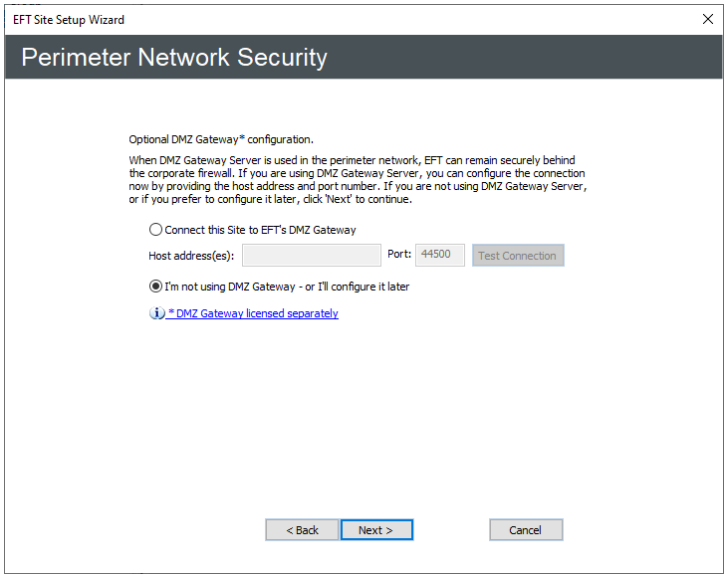
You change the refresh interval later in the Authentication Options dialog box.

13. If you will be using EFT with Azure Data-Lake Storage, next to **Override VFS Credentials**, click **Configure**. (You configure it later if you don't have the credentials available.) The **Override VFS Credentials**dialog box appears.

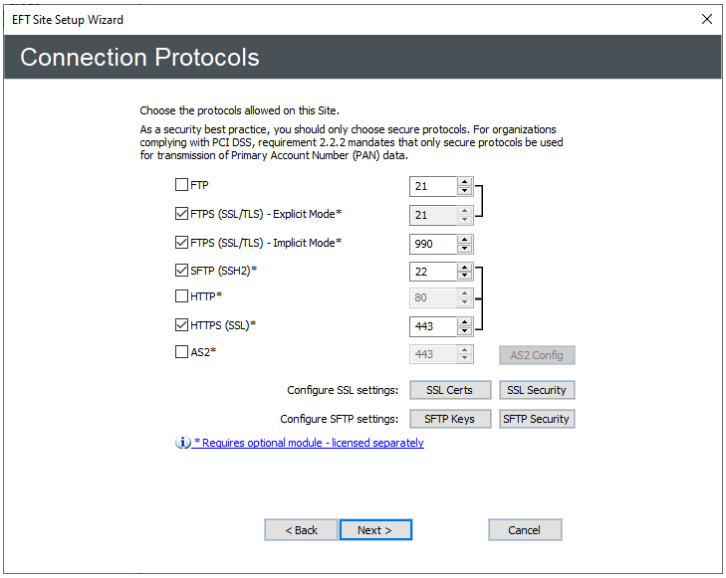


a. Select the **Enable VFS credentials override** check box. The **Login**and **Password** boxes become enabled.
b. Provide the credentials for your Azure Data-Lake supported container and the security key (password), then click **OK**.

14. Click **Next**. The **Perimeter Network Security**page appears.



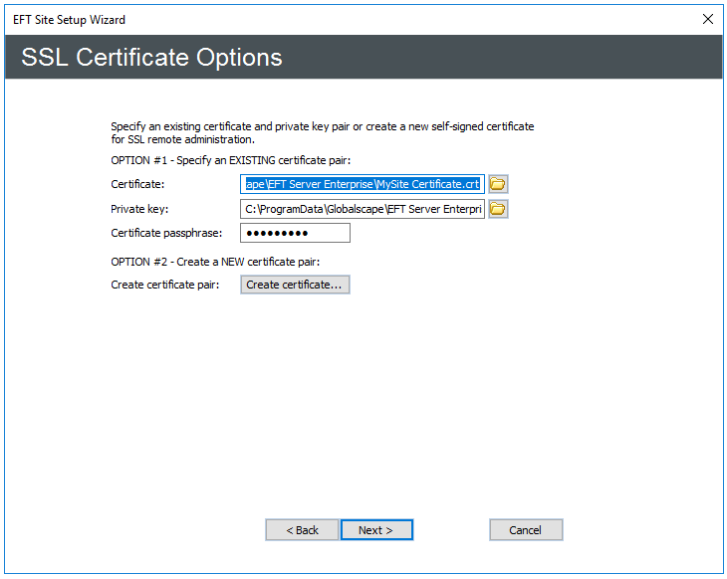
15. Specify whether to connect the Site to DMZ Gateway.
    - If you choose to connect to DMZ Gateway, specify its IP address and port, and then click **Test Connection**. If the DMZ Gateway is properly configured, the test is successful. If the test is not successful, click **I'm not using the DMZ Gateway - or I'll configure it later**.
    - If you have not yet installed or configured DMZ Gateway Server, click **I'm not using the DMZ Gateway - or I'll configure it later**.
16. Click **Next**. The **Connection Protocols** page appears.


EFT Site Setup Wizard
Connection Protocols
Choose the protocols allowed on this Site.
As a security best practice, you should only choose secure protocols. For organizations complying with PCI DSS, requirement 2.2.2 mandates that only secure protocols be used for transmission of Primary Account Number (PAN) data.
FTP
21
FTPS (SSL/TLS) - Explicit Mode*
21
FTPS (SSL/TLS) - Implicit Mode*
990
SFTP (SSH2)*
22
HTTP*
80
HTTPS (SSL)*
443
AS2*
443
AS2 Config
Configure SSL settings:
SSL Certs
SSL Security
Configure SFTP settings:
SFTP Keys
SFTP Security
* Requires optional module - licensed separately
< Back
Next >
Cancel

17. Select one or more check boxes for the protocol(s) that this Site will use to connect to EFT and specify the port number for each protocol. The default ports appear in the boxes.

    By default, the FTP server in Microsoft IIS binds to port 21 on all IP addresses. If you want to run both the IIS FTP server and EFT, you need to disable socket pooling for the IIS FTP server.

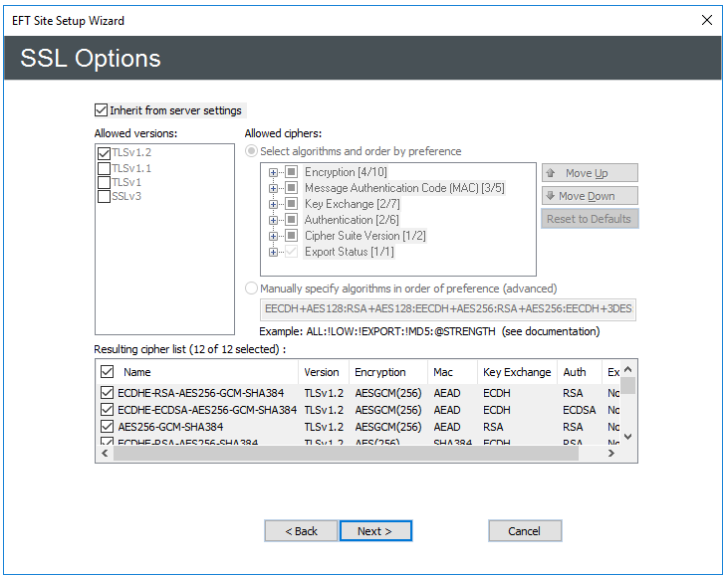
18. Specify the SSL certificate to use for this Site. Click **SSL certs**. The **SSL Certificate Options** page appears.



    - To create a certificate, click **Create certificate** and follow the prompts in the wizard. (Refer to Creating Certificates for details, if necessary.)
    - To use an existing certificate:
        i. In the **Certificate**box, type the path to the **.crt**file or click the folder icon to find and select it.
        ii. In the **Private key** box, type the path to the **.key**file or click the folder icon to find and select it.
        iii. In the **Certificate passphrase** and **Confirm passphrase** boxes, type and confirm the passphrase for the certificate pair.

    If you do not enable SSL, you will not be able to connect to EFT from a remote administration interface. Refer to SSL Certificate-Based Login, Creating Certificates and Importing a Certificate into the Trusted Certificate Databasefor information regarding certificates.

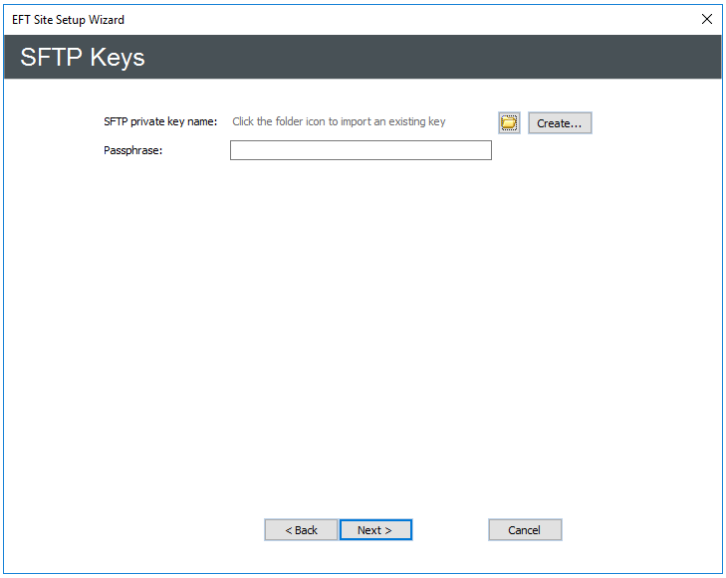
19. Click **Next**to return to the **Protocols**page.
20. If you are using SSL, click **SSL options**:



a. Select the **Inherit from server settings** check box if you want the Site to use the same configuration, or clear the check box to select different options.

b. TSLv1.2 is the only version selected by default in v8.0.5. Select other versions and/or ciphers as needed.

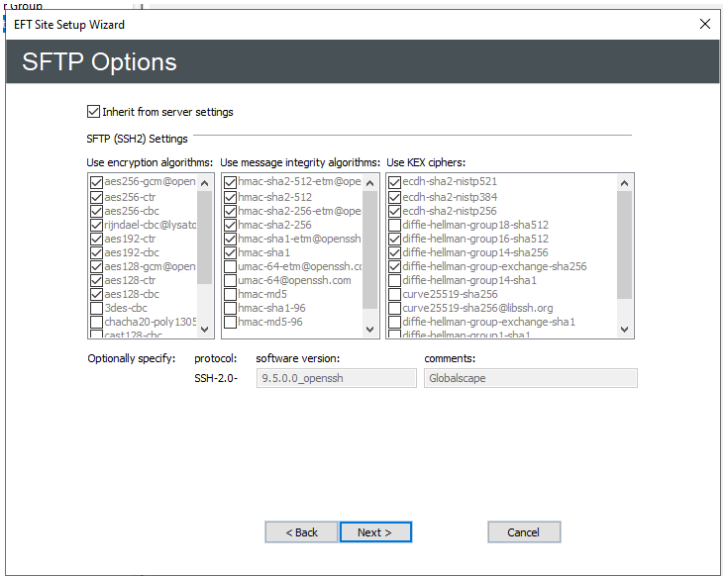
21. Click **Next**to return to the **Protocols**page.
22. (If you are using SFTP) Click **SFTP keys** to configure an SFTP key pair. The **SFTP Keys** wizard appears.



23. Do one of the following:
    - Click the folder to browse for a key, then enter the passphrase.

      -- or --

    - Click **Create**to create a new key. The **Create SSK2 Public/Private Keypair** wizard appears.
      a. Specify a name, location, format, and bit length of the key pair, and then click **Next**.
      b. Specify and confirm the passphrase to encrypt the private key, and then click **Next**.
      c. Specify whether to use this key as the default host key and whether to copy the public key to the SSH key manager, and then click **Finish**.
      d. After the key is generated, click **Finish**.
24. You are returned to the **Site Setup** wizard **Protocols**page. Click **SFTP Security**. The **SFTP Options** page appears.



25. (In v8.0.5 and later) Select the **Inherit options from server settings** to use the same configuration as the server, or clear the check box to select different options.
26. Select the algorithms and ciphers as needed, then click **Next**.
27. If you chose **AS2**, click **Configure**. The **AS2 Setup Wizard** appears. Click **Next**.

a. Specify **Your AS2 identifier**. There is no standard for the AS2 Identifier. You can use your name, your company's name, or some other unique name. EFT validates the AS2 identifier to determine whether it is unique (not used by another partner on this EFT). If you type an ID that is not unique, the field resets to blank. Click **Next**.

b. Specify the AS2 **Certificate public path key**, **Certificate private key path**, and **Certificate private key passphrase**, populated by default with the SSL certificate paths (if present) for EFT SSL communications. Click the folder icons to specify a certificate pair or click the blue **create** link to open the SSL certificate wizardto create a new certificate pair. (You can use the same SSL certificate that you are using for the Site.) Click **Next**.

c. Click **Finish**.

28. Click **Next**. The **Site Setup Completed** page appears.
29. If you specified Globalscape authentication, you are offered the option of running the user creation wizard or quitting the Site Setup wizard and creating users later. Click an option, then click **Finish**.
    - If you chose **Run New User Creation** wizard, the User Creation wizard **Welcome** page appears. Continue to Creating User Accounts for the procedure.

You can run the **Site Setup**wizard again at any time to create additional Sites.

You can view and modify individual Site settings in the administration interface.

Creating an Advanced Security Site

(Requires RCM.) When you run the Sitecreation wizard, you have the option to create a Site with "strict security" options enabled and that can monitor, report, and/or warn when those settings are changed and can cause compliance violations.

Prerequisites:

- Auditing and Reporting module enabled
- Regulatory Compliance Module activated or in trial

Constraints:

- Authentication not allowed using SSL certificate or SFTP key-only

For details of configuring Servers and Sites, and enabling ARM on EFT, refer to the following topics:

- Server Setup Wizard
- Configuring the Auditing and Reporting Module

You will need the following information to create and configure a "strict-security" enabled Site:

- Listening IP address for the Site
- Site root folder path (location)
- User authentication provider type
- DMZ Gateway IP address and port, if applicable
- The email address for emailing the PCI DSS Compliance Report
- SSL certificate pair and SFTP key pair if applicable

The wizard performs several checks and asks you to provide information or make changes based on the results of those checks, including:

- Is the RCM in the trial period?
- If not in trial period, is the module activated?
- Is ARMenabled?
- Which authentication method are you using to authenticate users?
- Is remote administration enabled?
- Is SSL enabled for remote administration?
- Are password security options for delegated administration set?
- Is the daily PCI DSS report enabled?

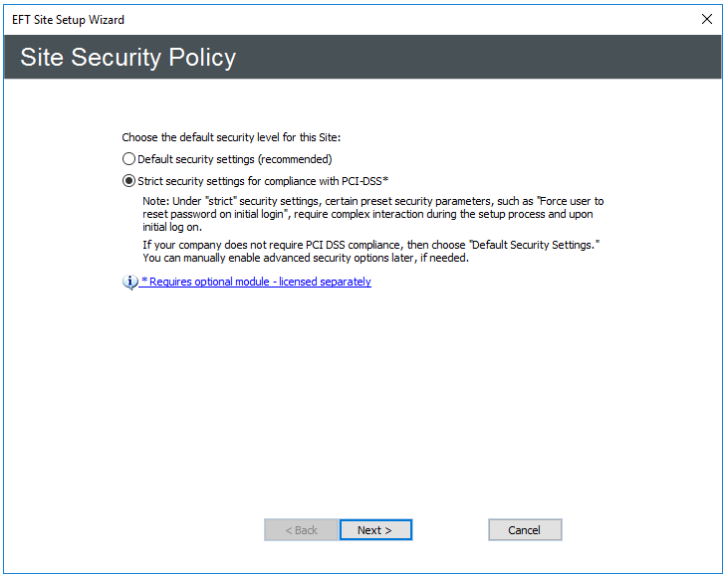
- Is FTPS/HTTPS/SFTP enabled?
- Is the default banner for SFTP used?

The wizard is quite intuitive and provides instructions where necessary. The wizard pages change based on your selections. The procedure below walks you through the most common scenarios.

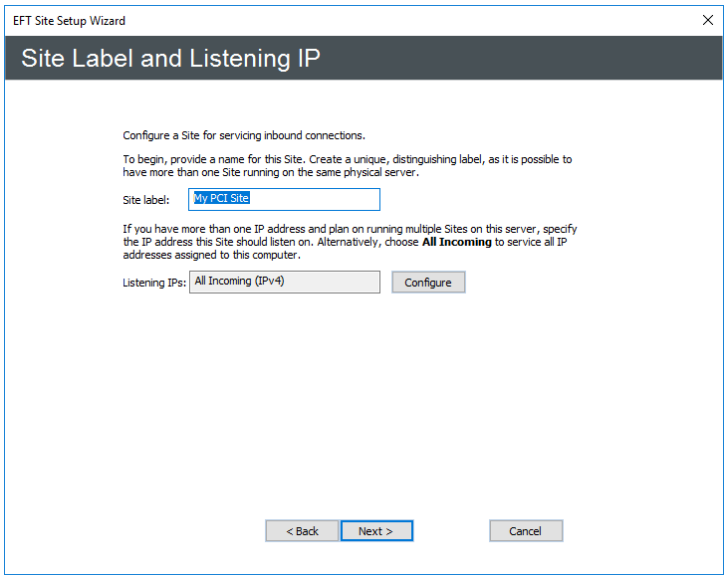
To configure a strict-security enabled Site

1. Do one of the following:
   - After Server setup is complete, the **Site Setup**wizard appears.
   - In the administration interface, click **Configuration >New Site**.

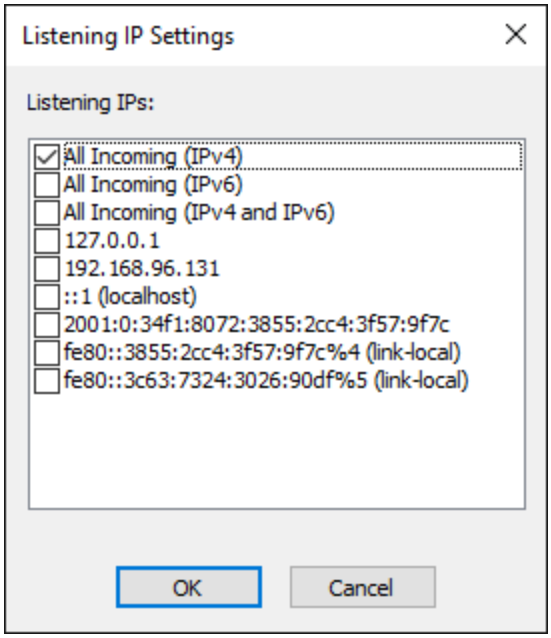
   The **Site Setup** wizard **Site Security Policy** page appears.



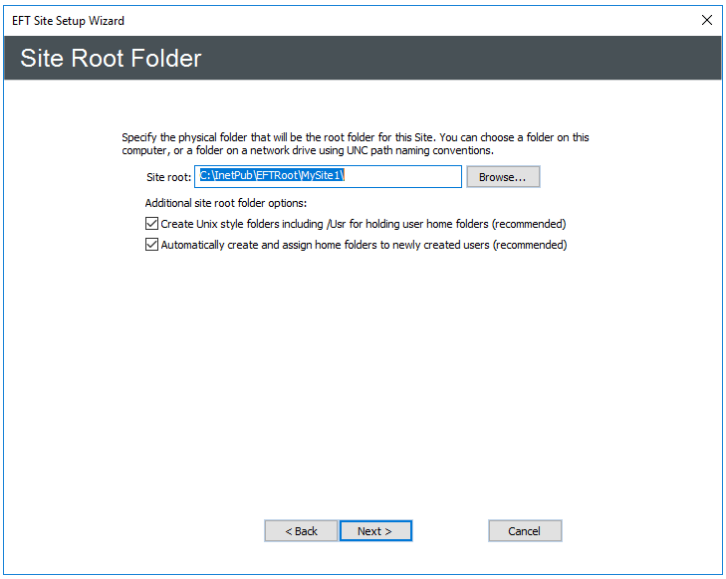
2. Click **Strict security settings**, and then click **Next**. The **Site Label and Listening IP**page appears.



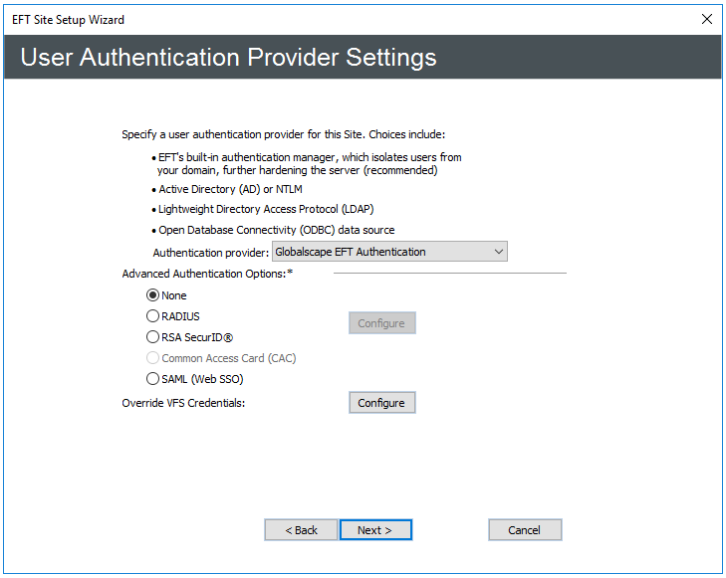
3. In the **Site label**box, type a name a unique name for the Site. The default name is MySite, but you can change it to anything you want. The name you provide here will appear in the EFT tree in the left pane of the administration interface and in reports and messages.
4. Next to the **Listening IPs** box, click **Configure**. The **Listening IP Settings**dialog box appears.



5. Select one of the **All Incoming** check boxes, or one or more specific IP addresses on which this Site should listen for incoming connections, and then click **OK**.
6. Click **Next**. The **Site Root Folder** page appears.



7. In the **Site root**box, leave the default or click **Browse**to specify the root folder. For HA cluster configured Sites, the Site root is in the HA shared configuration folder.
8. In the **Additional site root folder options** area, select or clear the check boxes as needed:
    - Select the **Create UNIX-style subfolders including /Usr for holding user home folders**check box with appropriate permissions under the Site root folder. This is only necessary if you are trying to mimic a typical default *nix Server setup, but the check box is selected by default.
    - Select the **Automatically create and assign home folders to newly created users** check box to create a user folder automatically under **/Site Root/Usr/** when a new user is added.
9. Click **Next**. The **User Authentication** page appears.



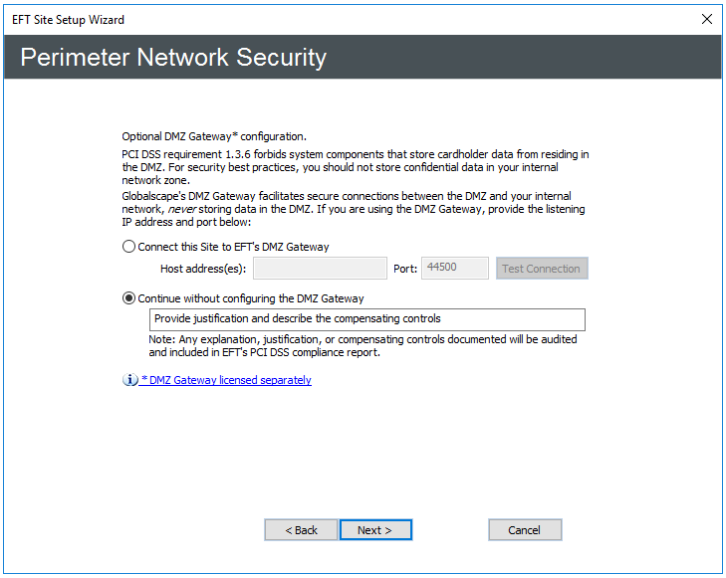
10. In the **Authentication type** list, specify one of the following authentication methods that this Site will use to authenticate user connections:
    - **Globalscape EFT Authentication**
    - **Windows Active Directory Authentication** - If you are using this method, also refer to Windows Active Directory Authentication.
        - If you are using Active Directory with RADIUSor RSA SecurID, click the applicable option and then click Configure to configure the RSA or RADIUS settings.
    - **LDAP Authentication**- If you are using this method, also refer to LDAP Authentication.
    - **ODBC authentication**- If you are using ODBC authentication, also refer to ODBC Authentication.

    When you create a high security-enabled Site that uses **AD** or **LDAP** authentication, the following states will not be audited for user accounts, but will be audited for non-AD administrator accounts:
    - Password complexity and length requirements
    - Password history requirements
    - Password reset requirements
    - Password expiration requirements
    - Password anonymous requirements
    - Password emailing to user requirements

    The same PCI DSS requirement checks are skipped when RADIUS or RSA SecurID is used, and compensating controls are shown in their place.
11. Under **Advanced Authentication Options**, specify whether this Site will use **RADIUS**, **RSA SecurID**, **SAML (Web SSO)**, **OpenID**, or the default of **None**. (**Common Access Card (CAC)** authentication is not allowed for strict-security enabled Sites.)
    - If **RADIUS**, **RSA SecurID**, **SAML**, or **OpenID** is selected, click **Configure**, then:
        - RADIUS - Specify the RADIUS authentication settings, and then click **OK**.
        - RSA SecurID - Specify the location of the RSA Server configuration file (**sdconf.rec**), then click **OK**. (Note that SecurID files will reside in this location. Node secret and sdstatus.12 files will be generated at this location.)
        - SAML (WebSSO)- Click **Configure** then refer to Configuring a Site for SAML.
        - OpenID - Click **Configure** then refer to OpenID Configuration.

- (Optional) Next to **Override VFS Credentials**, click **Configure**. Enable and provide login information, if needed. (Refer to Override VFS Credentialsfor details of this option.)

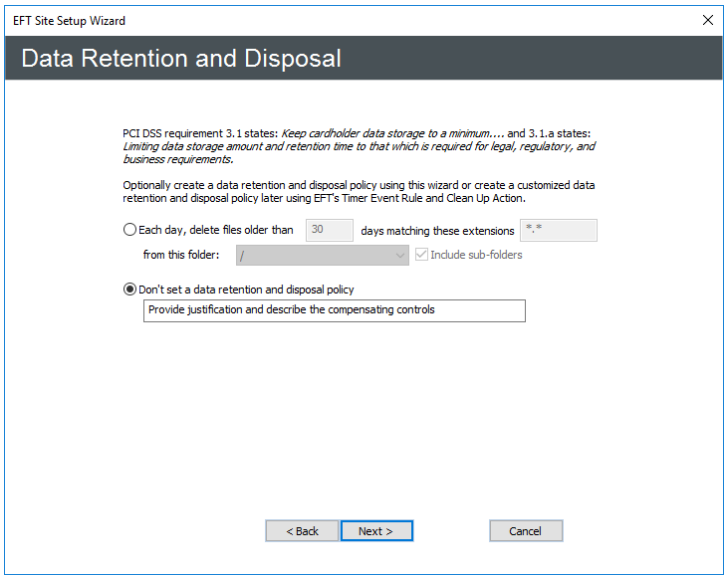
12. Click **Next**. The **Perimeter Network Security**page appears.



13. If you are using the DMZ Gateway module, provide the IP address and port to connect the Site to DMZ Gateway, then click **Test Connection** to verify that the Site can connect to DMZ Gateway. If the Site is unable to connect, you can continue without enabling DMZ Gateway and enable it later.
    - If you choose not to connect to DMZ Gateway or have not yet installed DMZ Gateway, click in the text box and provide a reason (compensating control) for not using DMZ Gateway. (The reason will appear in the **Description**box of the PCI DSS Compliance report.)
14. Click **Next**.
    - If you specified a default port for DMZ Gateway, the **Vendor Defaults** page appears. Change the port number to a non-default number, or provide a reason for keeping the default port. (The reason will appear in the **Description** box of the PCI DSS Compliance report.)

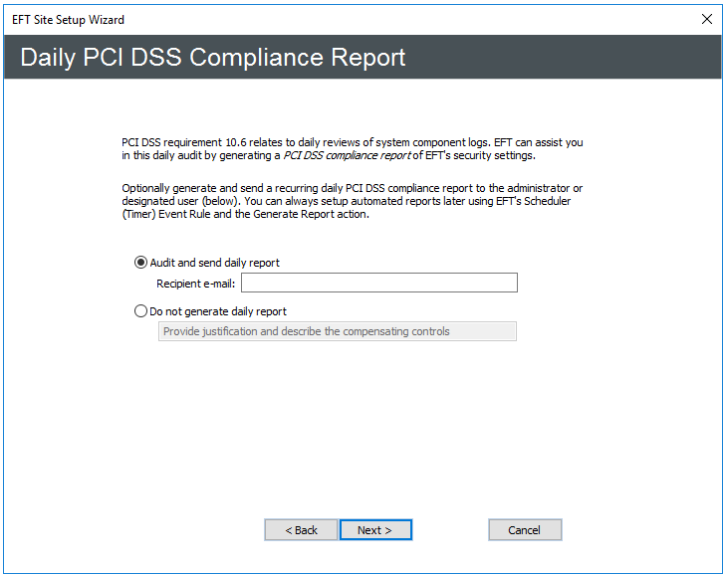
      - OR -

    - The **Data Retention and Disposal** page appears.

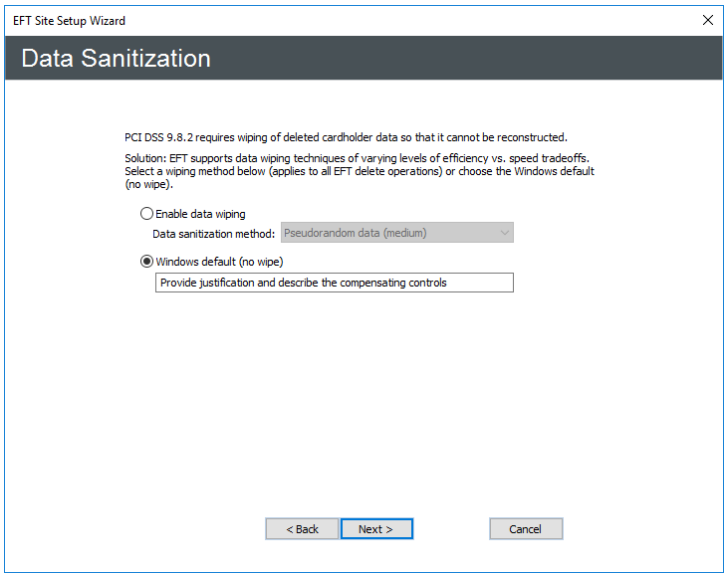


15. Do one of the following:
    - Click **Each day, delete file older than n days matching these extensions from this folder**, then specify the file extensions to be deleted, the frequency, and the folder from which to delete them. Select the **Include subfolders**check box to delete the files from the subfolders.
    - Click **Don't set a data retention and disposal policy**, then, in the text box, provide the justification and compensating control. (The reason will appear in the **Description**box of the PCI DSS Compliance report.) Refer to Specifying File Deletion Options for more data wiping options. You can always setup a clean-up policy later.
16. Click **Next**. The **Administrator Account Password Security** page appears.

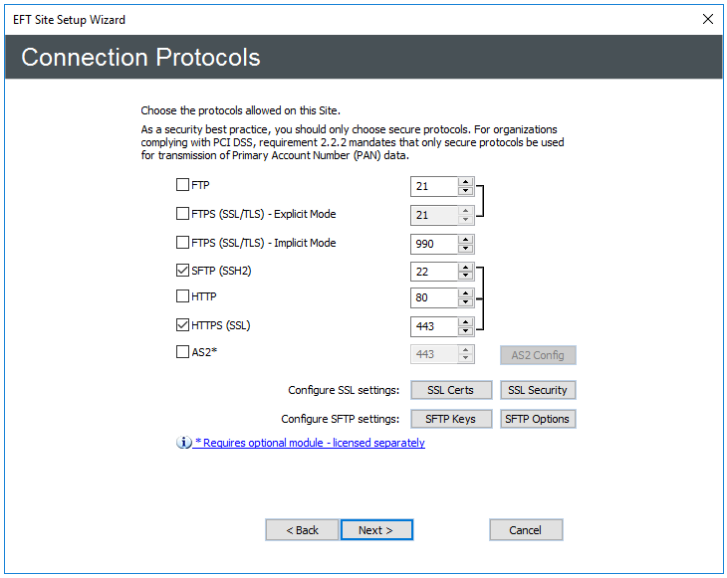
17. Keep the default of **Enable options identified above for all administrator accounts** (password security settings) or click **Continue without changing administrator account password security settings**, then provide the justification and compensating control. (The reason will appear in the **Description**box of the PCI DSS Compliance report.) You can specify these password security settings individually after you create the Site.
18. Click **Next**. The **Daily PCI DSS Audit Report**page appears.



19. Do one of the following:
    - Click **Audit and send daily report**, then provide the recipient's email address. (The SMTP settings were configured during Server setup.)
    - Click **Do not generate daily report** and type a reason for not generating the report automatically. For example, you can manually generate the report as needed in the administration interface. (The reason will appear in the **Description**box of the PCI DSS Compliance report.)
20. Click **Next**. The **Data Sanitization** page appears.



21. Do one of the following:
    - Click **Enable data wiping**, then, in the **Data sanitization method** box, click which method EFT is to use to wipe data.
    - Click **Windows default (no wipe)** and type a reason for not specifying a data sanitization method for EFT to use. For example, you might be using a third-party tool for sanitization. (The reason will appear in the **Description**box of the PCI DSS Compliance report.)
22. Click **Next**. The **Connection Protocols**page appears.

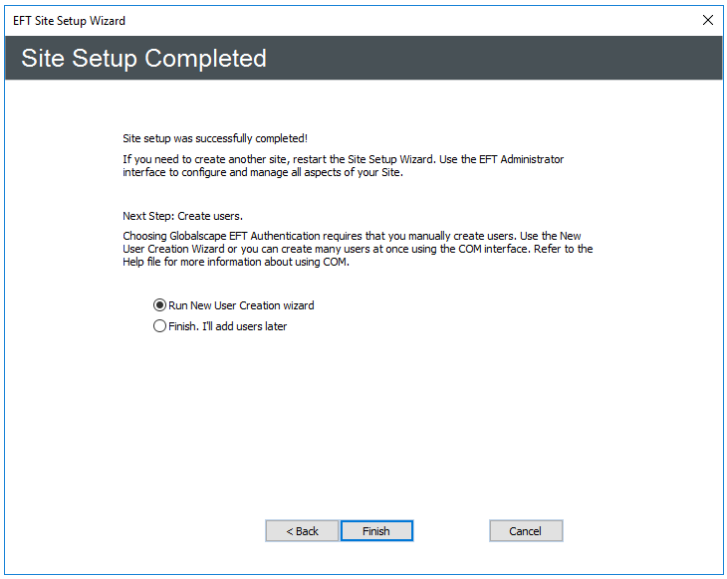


23. Select one or more protocol check boxes and specify the port numbers that this Site will use to connect to EFT. If you specify plain text FTP or HTTP, after you click **Next**, EFT will prompt you to disable these insecure protocols or

continue and supply justification.

- If you choose **SSL**, click **SSL options** and **SSL certs** for further configuration.
  - Click **SSL options** to define the allowed SSL versions and ciphers. Some Web browsers do not have TLS turned on by default, which causes things like redirecting to the password reset page to fail, because the browser cannot make the SSL connection, and it returns an error. For this reason, default SSL security options for a high security-enabled Site include SSL 3.0 in addition to TLS 1.0.
  - Click **SSL certs** to define the SSL certificate to use for this Site. Refer to Creating Certificates and Importing a Certificate into the Trusted Certificate Database for information regarding certificates.
  - Regarding SSL certificate-based login, compliance with PCI DSS requires that users change their password upon initial login. Because SSL certificate-only login does not use a password, it potentially violates the PCI DSS and is, therefore, not available with high security-enabled Sites.
- If you choose **SFTP**, click **SFTP options** and **SFTP keys** for further configuration. Because the SFTP **Public key only** method does not use a password, it potentially violates the PCI DSS and is, therefore, not available with high security-enabled Sites. However, you can use the **Public Key and Password** authentication method.
- If you choose **AS2 over HTTP/S**, click **Configure**to specify your AS2 identifier and certificate information.

24. Click **Next**. If the default SFTP banner message is used on EFT, the **Vendor Default** warning page appears. Do one of the following:
    - Click **Change SFTP message banner to**, then provide the software version and, optionally, comments.
    - Click **Continue without making any changes**, then type the reason for keeping the default banner message.
25. Click **Next**. The **Site Setup Completed** page appears.



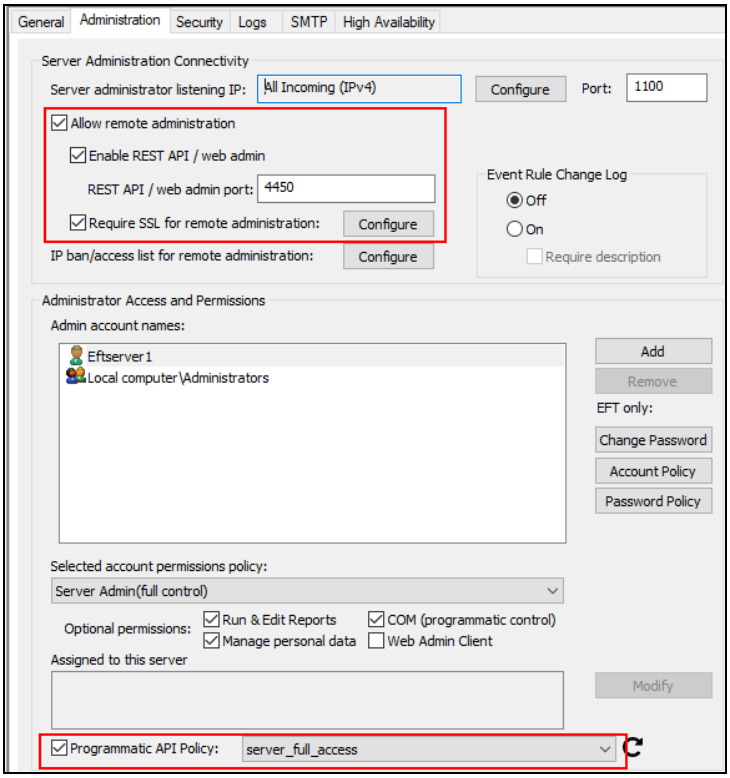
26. You are offered the option of continuing to the User Creation wizard or quitting the wizard. Click an option, and then click **Finish**. The high security-enabled Site appears in the tree on the **Server**tab.
    - If you chose **Run New User Creation** wizard, the User Creation wizard **Welcome**page appears.

Propagating an EFT Site

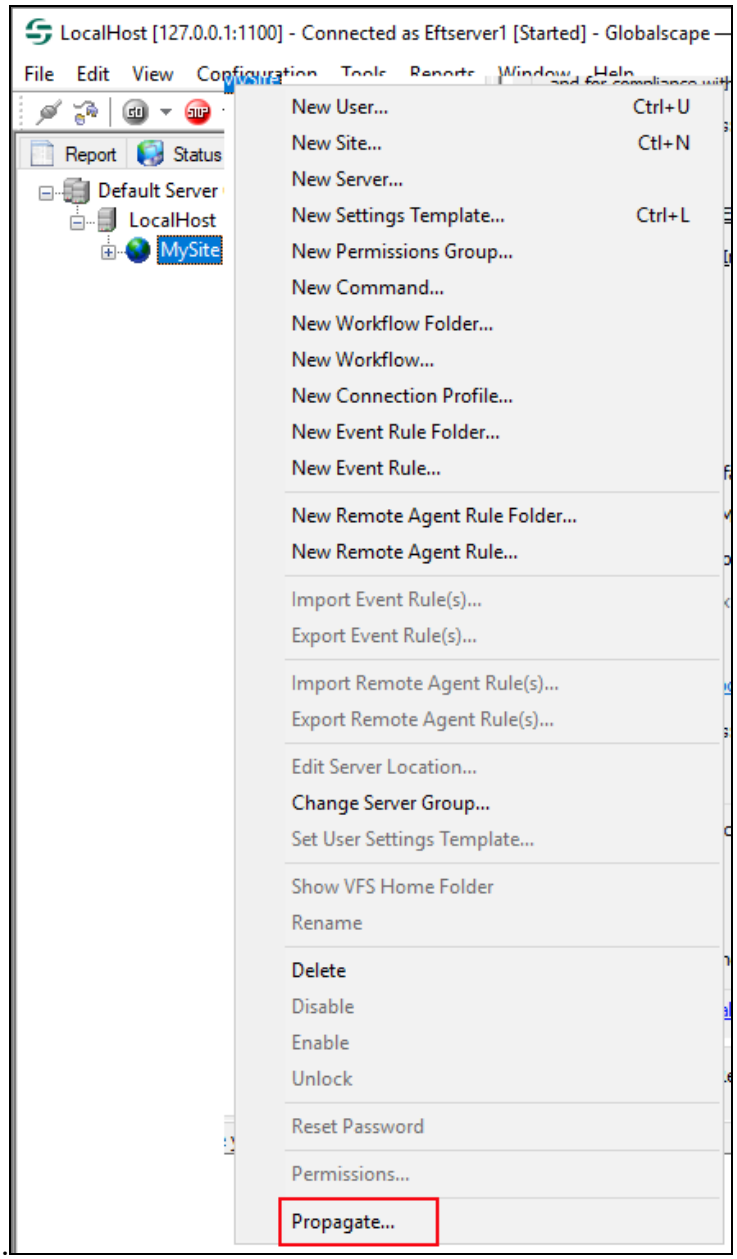
For disaster recovery, some customers need to perform a unidirectional sync across settings from a live EFT site to another so that a backup system is available.

To propagate an EFT Site

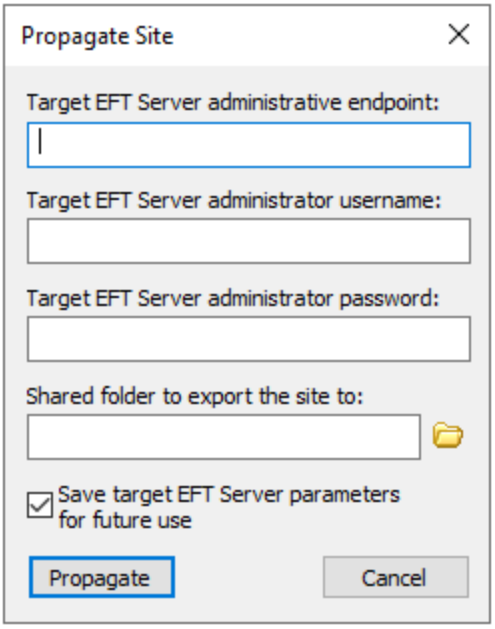
- Internally, propagation is performed via target server's REST Administrator interface, so target server must have Web-admin enabled for the feature to work.
- The administrator must be at least a Site-level Administrator.
- Administrator account must have **Programmatic API Policy** enabled.
- The production and backup servers must have similar (or same) environments (file system structure, network neighborhood, and so on).
- Both servers must use the same run-time variables to configure environment-specific parameters.



- On the **Server** tab, right-click the Site node, then click **Propagate.**



The **Propagate Site** dialog box appears. Provide the target EFT Server details and a shared folder in which to export the Site, then click **Propagate**.



- **Target EFT Server administrative endpoint**. URL:port such as https://192.168.118.128:4450.
- **Target EFT Server administrator username** and **password** (EFT managed accounts only; there is no AD/LDAP support for administrator accounts in this dialog).
- **Shared folder to export the site to.** The target server, receiving server, and the EFT Server service must each have an account that has read/write access to the shared folder.
- Select the **Save target**... check box to save the propagation parameters for future reuse. If selected, after successful propagation,
- All the parameters except for target server administration password are preserved across EFT administrator interface restart
- Target server administration password is preserved during current EFT administrator interface session

  The identity is provided by an internal site ID:

  - If target server had no site with matching ID, the site is created.
  - If target server had the site with matching ID, it is replaced.

The following parts of the site are propagated:

Whole configuration database

- Except for node-specific parameters (“replace existing” scenario)
    - Started/stopped status
    - Listen IP
    - DMZ gateway settings
- If the value of a filesystem-related parameter of source server site points to source server Configuration Directory (by default, C:\ProgramData\Globalscape\EFT Server\ for standalone deployment and HA cluster share for HA deployment), then the value of target server site points to the target server Configuration Directory
    - The filesystem-related parameters are:
        - Server SSL certificate and key
        - DMZ Gateway SSL certificate
        - DMZ internal SSL certificate and key
        - SAML IdP certificate
        - AS2 certificate and key
        - AS2 Inbound/outbound partners’ certificates
- For example, if a site of standalone-deployed source server is configured to use SSL certificate C:\ProgramData\Globalscape\EFT Server\Certificates\ssl.crt, then, after site propagation, the site of HA-deployed target server is configured to use SSL certificate <CLUSTER_SHARE>\Certificates\ssl.crt

Site files

- Server SSL certificate and key
- DMZ Gateway SSL certificate (only in “create new” scenario as it is a part of node-specific parameters which are preserved in “replace existing” scenario)
- DMZ *internal* SSL certificate and key
- SAML IdP certificate
- AS2 certificate and key
- AS2 Inbound/outbound partners’ certificates
- Email templates
- HTML templates
- WTC customization files

Files are propagated path-to-path, i.e., the file located at <PATH> at the source server is propagated to the <PATH> at the target server, except for the files located in Configuration Directory, HTML/email Template Directory, and WTC Customization Directory, which are propagated to the corresponding directory at the target server

- For “replace existing” scenario, the target server backs up and removes the entire existing WTC Customization Directory
- For “replace existing” scenario, the target server backs up and removes all HTML/Email template files

For any other file, if a corresponding file already exists at target server:

- For “create new” scenario, propagation fails (as it means that the file belongs to other site/service and it is unclear how to handle their propagation)
- For “replace existing” scenario, EFT backs up the existing file and replaces it with up-to-date version from target server

The following parts of site are not propagated:

- Admin ACLs
- Site file system objects (physical files and folders)
- Referenced external objects like Custom Command Executable, PowerShell Scripts, etc
- SDConf.rec (RSA Securid config)

For site propagation to succeed, the specified target server's administrator credentials should correspond to the Server-level (to create new site) or Site-level administrator target server administrator (to replace existing site) of target server.

- Site propagation fails if source or target server has `SecretsModuleEncryptionKey` Advanced Property defined
- Source server records propagation progress to EFT.log via COMMON logger
- Target server records propagation progress to EFT.log via COMMON logger
- Target server registers propagation to ARM database as Admin Activity
- Site.Created, for “create new” scenario
- Site.Replaced, for “replace existing” scenario
- Target server does not perform PCI audit when accepting site propagation
- Site propagation is available via COM admin interface, ICISite::Propagate method
- Site propagation is available via REST Admin interface; the request is POST to /Admin/v2/sites/<site-id> . The semantics of requests is RPC, and it is implemented based on JSON-RPC protocol (https://www.jsonrpc.org/specification) rather than in “standard” JSON:API model. The method name is “propagate.”

Success Case Example:

```
POST /Admin/v2/sites/00000000-0000-0000-0000-000000000001 HTTP/1.1

{

    "jsonrpc": "2.0",

    "method": "propagate",

    "id": "1",

    "params":
    {

        "targetEndpoint": "http://target:4450",

        "exportDirectoryPath": "\\\\server\\Share\\4SitePropagation",

        "targetAdminUsername": "targetAdminLogin",

        "targetAdminPassword": "targetAdminPassword"

    }
}

    HTTP/1.1 200 OK
    {
        "jsonrpc": "2.0",
        "id": "1",
        "result": "success"
    }
```

Failure Case Example:

```
POST /Admin/v2/sites/00000000-0000-0000-0000-000000000001/custom-commands/00000000-0000-0000-0000-000000000001 HTTP/1.1

{

    "jsonrpc": "2.0",

    "method": "propagate",

    "id": "1",

    "params":
    {

        "targetEndpoint": "http://target:4450",

        "exportDirectoryPath": "\\\\server\\Share\\4SitePropagation",

        "targetAdminUsername": "targetAdminLogin",

        "targetAdminPassword": "targetAdminPassword"

    }
}

HTTP/1.1 500 Internal Error

{

    "jsonrpc": "2.0",

    "id": "1",

    "error":
    {

        "code": -32000,

        "message": "Server error: Unauthorized request"

    }
}
```

Starting or Stopping a Site

You might occasionally need to stop and restart a Site, such as when you create and assign a certificate to a Site or configure the DMZ Gateway to connect to a Site.

Occasionally, EFT might get a "false positive" indication that ports are in use when attempting to start the Site, preventing the Site from starting. To avoid this, you can enable advanced properties to delay Site start, retry start, or retry start after a defined delay. Refer to the Knowledgebase article for details: https://kb.globalscape.com/KnowledgebaseArticle11450.aspx

To start or stop a Site

When you stop the Site, EFT breaks all existing connections and waits until all socket threads die. The service can terminate when Timer Event processing is still in progress. The triggering of Monitor Folder and Timer Event Rules occurs almost simultaneously and is controlled by the operating system, not by EFT. Refer to Event Rule Order of Execution for more information.

1. In the administration interface, connect to EFT, and then click the **Server** tab.
2. On the **Server**tab, click the Site that you want to start or stop.
3. In the right pane, click the **General**tab.
4. In the **Statistics**area, do one of the following:
    - Click **Stop**. The **Site status** changes to **Stopped**.
    - Click **Start**. The **Site Status** changes to **Started**.

FTP/S

The FTP and FTPS protocols can be enabled/configured on the Site and inherited by the Settings Templates and user accounts. (You can then configure the Settings Templates and user accounts differently, if needed.) The topics below provide the procedures for configuring FTP/S settings on Sites, Settings Templates, and user accounts.

- Allowing Site-to-Site Transfers (FXP)
- Allowing Client Anti-Timeout Schemes (NOOP)
- Allowing Multipart Transfers (COMB Command)
- Allowing the Mode Z Command
- Configuring FTP or FTPS
- Connections Settings
- EFT Support for EBCDIC
- Encoding for FTP Transfers
- File Integrity Checking (XCRC)
- FTP Commands Supported by the Server
- Specifying a PASV IP or PASV Port Range
- Specifying the Value Returned by the FTP SYST Command

Allowing Site-to-Site Transfers (FXP)

Although site-to-site transfers (FXP command) can expedite what otherwise could be a slow transfer, many administrators consider site-to-site transfers a security risk, exposing servers to "port theft" or "FTP by proxy" attacks. Depending on how your servers are configured, you might want to block these types of transfers.

To allow or block Site-to-Site transfers

1. Open the **FTP Settings** dialog box.
2. Do one of the following:
   - To allow transfers, select the **Allow site-to-site transfers (FXP)** check box.
   - To block transfers, clear the **Allow site-to-site transfers (FXP)** check box.
3. Click **OK** to close the **FTP Settings** dialog box.
4. Click **Apply** to save the changes on EFT.

Allowing Client Anti-Timeout Schemes (NOOP)

Many FTP clients send random commands such as REST 0, PWD, TYPE A, LIST, etc., to the FTP server to keep the session alive while the client is idle. Many FTP clients send a NOOP command to EFT during idle times to keep the connection alive. You can choose whether to allow the NOOP command. If you disallow the NOOP command, it will be considered an invalid command and treated according to your settings under **Disconnect after <n> invalid commands**.

To allow or disallow the NOOP command

1. Open the **FTP Settings** dialog box.
2. Select the **Allow FTP client anti-timeout schemes** check box to allow the NOOP command or clear the check box to treat the NOOP command as an invalid command. (Selected by default.)

   If you are banning users who send excessive invalid commands while treating NOOP as an invalid command, then you will be banning users for sending the NOOP command. You may later allow the user to connect by removing their IP address from the Site's list in the **IP Access** tab. A gray check box in a user account indicates that the account is inheriting parameters from the Settings Template.

3. Click **OK** to close the dialog box.
4. Click **Apply** to save the changes on EFT.

Allowing Multipart Transfers (COMB Command)

EFT supports multi-part transfers from advanced FTP clients such as CuteFTP. The user must have appropriate privileges and be authorized to connect multiple times Allowing Multipart Transfers (COMB Command). The connecting client takes care of most details, including splitting the file apart, sending the multiple parts, and then requesting that the Server to join them again upon receipt.

To allow or block multipart transfers

1. Open the **FTP Settings** dialog box.
2. Do one of the following:
   - To allow transfers, select the **Allow multi-part transfers (COMB)** check box.
   - To block transfers, clear the **Allow multi-part transfers (COMB)** check box.
3. Click **OK** to close the **FTP Settings** dialog box.
4. Click **Apply** to save the changes on EFT.

How does the COMB command work?

The COMB command joins the parts back together. The benefits of segmented (multi-part) and concurrent delivery for accelerated transfers include:

- Accelerate throughput and maximize available bandwidth available to the client by allowing uploaded files to be split apart and transferred in multiple segments simultaneously.
- Command can be toggled on or off.

The COMB command is a proprietary command and is not defined nor endorsed by any FTP-related RFC; however, the command can be integrated with other servers using the following syntax:

```
COMB <TF> <SF 1> ... <SF n>
```

where

<TF> is the path to target file, which will contain the combined data from the source parts.

<SF #> are the source files (parts).

Which means combine ***n*** source files (SF 1...***n***) into one file (TF).

Notes regarding the COMB command:

- If the target file already exists, then EFT appends source files to it.
- EFT will delete all the source files once they are combined successfully.
- All file names should be in quotation marks.
- Upload, download, append, and delete permissions are REQUIRED, otherwise COMB will fail.
    - Upload and Append permissions are checked for the target result file.
    - Download and Delete permissions are checked for the source parts that are read for the COMB into the target result file.
    - Cleanup (delete) is performed on the target result file if an error occurs accessing the source parts.

Examples of using the COMB command:

- You can append a single part onto an existing (or new) file: e.g., COMB "final.log" "132.log".
- Paths are accepted for the target filename, but not for source parts file path. For example:
    - COMB "boslin/blah/final.log" "70.log" "71.log" "72.log" "73.log"
- There is no limit to the number of parts, but there is a server-side processing limit of approximately 1024 characters.
- A space is not required between quote-delimited file names. For example:
    - COMB "final3.log""60.log"
    - COMB COMB "final3.log" "60.log"
- Target and source files do not require enclosing quotes UNLESS the filename includes spaces. In that case you should use quotes. For example:
    - The following syntax is correct:
        - COMB final5.log 64.log 65.log
        - COMB “final5.log” “64.log” “65.log”
        - COMB final7.log "6 6.log" 67.log
    - The following syntax will not work because the filename includes spaces:
        - COMB final6.log 6 6.log 67.log

Allowing the Mode Z Command

Mode Z compression compresses files on the fly for file transfers, saving bandwidth and improving transfer times. The client must also support MODE Z to take advantage of this feature. If MODE Z is enabled, EFT will listen for MODE Z requests, then enable it for subsequent transfers from the client that requested it.

To allow a client to use Mode Z compression

1. Open the **FTP Settings** dialog box.
2. Select the **Allow MODE Z Compression** check box.
3. Click **OK** to close the **FTP Settings** dialog box.
4. Click **Apply** to save the changes on EFT.

Configuring FTP or FTPS

If you specify plain-text FTP or HTTP for a Site created using the "strict security settings" option, EFT prompts you to disable these insecure protocols, or continue with reason.

The FTP protocol is an interactive file-transfer mechanism that enables file transfers between Internet sites, or, more specifically, between two systems. It was created for transferring files independently of the operating system used, for example between a Macintosh and Windows PC. FTP's more notable features include handling for specific error situations and ensuring that a file sent from point A to point B will get there reliably.

The FTP protocol specification (RFC 959) was published many years ago when security was not a priority issue. As security became a concern, secure mechanisms such as SSL and TLS were adapted to help protect the FTP session from being intercepted or exploited. EFT provides security with FTPS (using SSL/TLS).

FTP Settings Dialog Box

The **FTP Settings** dialog box is used to allow or deny various FTP commands on a Site, Settings Template, or user account. The available options on the Site's FTP Settings dialog box differ slightly from the options on the Settings Template/user dialog box.

You can configure FTP connections to the Site on the Site's **Connections**tab. You can enable or disable FTP transfers at the Site, Setting Template, or per user.

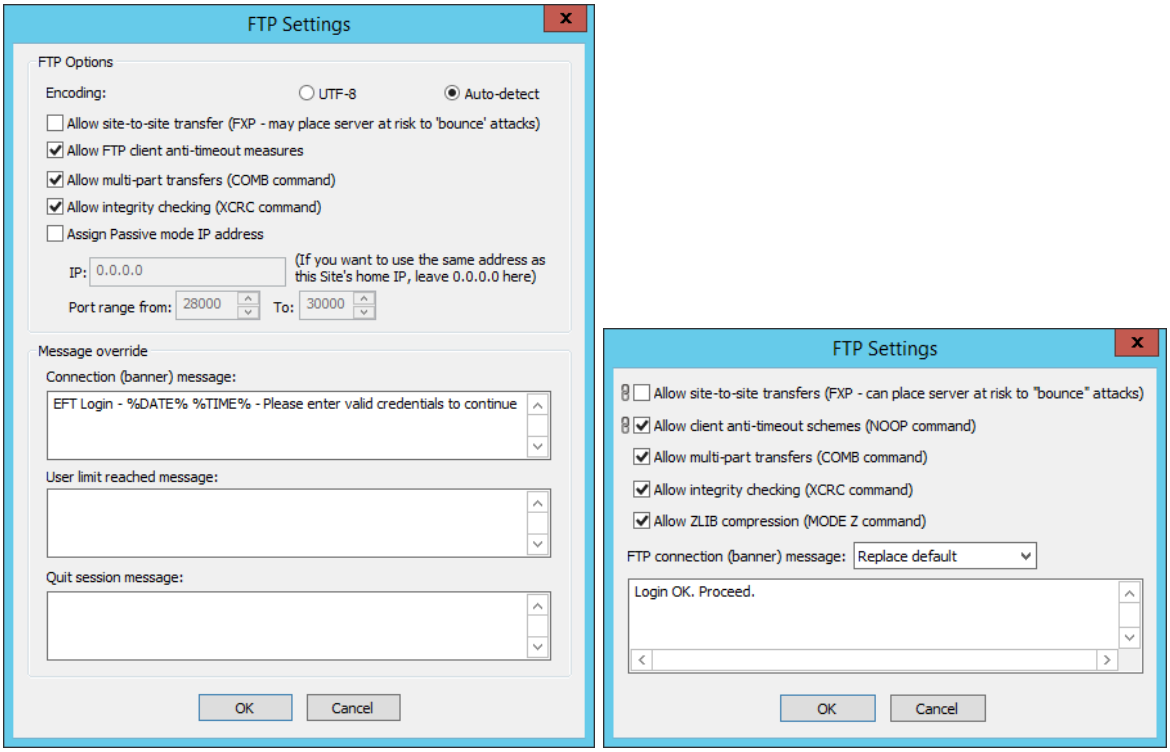
For information about how to configure your firewall to allow FTPS connections to EFT, refer to your firewall's user guide or knowledge base.

FTP requires UPLOAD permission in addition to APPEND to resume a partial file transfer.

To open the FTP Settings dialog box

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site, Settings Template, or user account that you want to configure.
3. In the right pane, click the **Connections**tab.
4. Select the **FTP**, **FTPS (SSL/TLS) - Explicit**, or **FTPS (SSL/TLS) - Implicit**check box. (See also Configuring SSL on the Server.)
5. Specify the port used for the connection (by default, 21 for plain FTP or 990 for FTPS Implicit).

6. Click **FTP/S Configure**(on the Site's **Connection**tab) or **FTP Config** (on the Settings Template's or user account's **Connection**tab). The **FTP Settings** dialog box appears.



Refer to the linked procedures below for details of each option:

- Encoding for FTP Transfers
- Allowing Site-to-Site Transfers (FXP)
- Allowing Client Anti-Timeout Schemes (NOOP)
- Allowing Multipart Transfers (COMB Command)
- File Integrity Checking (XCRC)
- Allowing ZLIB Compression (Mode Z)
- Specifying a PASV IP or PASV Port Range
- Connection Banner Message
- User Limit Reached Message
- Quit Session Messages

EFT Support for EBCDIC

Extended Binary Coded Decimal Interchange Code (EBCDIC) is an 8-bit character encoding used on IBM mainframe operating systems such as z/OS, OS/390, VM and VSE, IBM midrange computer operating systems such as OS/400 and i5/OS, and on various non-IBM platforms such as Fujitsu-Siemens' BS2000/OSD, HP MPE/iX, and Unisys MCP.

EFT complies with TYPE E (EBCDIC) mode for FTP-based file transfers (in server mode):

- When a client or mainframe uploads a file over FTP/S and requests TYPE E, EFT converts the file to ASCII (native Windows format).
- When a client or mainframe downloads a file and requests TYPE E, EFT converts the file into EBCDIC format and sends it to the requesting client.

EFT supports conversion of ASCII to EBCDIC and vice versa. Unfortunately, there are several “standard” mappings and EFT currently supports only one of them, the one recommended by Microsoft and IBM.

The table linked below is an ASCII-to-EBCDIC conversion table that translates 7-bit ASCII characters to 8-bit EBCDIC characters. This translation is not bidirectional. Some EBCDIC characters cannot be translated to ASCII and some conversion irregularities exist in the table.

https://www.ibm.com/docs/en/iis/11.3?topic=tables-ascii-ebcdic

> **NOTE:** EFT does not support the HP standard (used by the dd tool in Linux).

Encoding for FTP Transfers

Support for UTF-8 encoding is communicated in response to the FEAT command, which occurs after authentication. Therefore, if you provide a Unicode username/password and try to connect to the server via FTP, the connection will fail. EFT starts negotiation in ASCII and can't switch to Unicode until after authentication. If you want EFT to use Unicode from the start, you can change the initial encoding in the interface in the **FTP Settings** dialog box.

You can specify **UTF-8** or **Auto-detect** encoding for inbound FTP transfers on the Site. For most connecting clients, **Auto-detect** is preferred and is the default.

To configure FTP encoding

1. Open the **FTP Settings** dialog box.
2. In the **Encoding** area, click **UTF-8** or **Auto-detect**.
    - **UTF-8**—For Unicode-only transfers
    - **Auto-detect**—Detects whether to proceed in ASCII mode or can switch to UTF-8 mode for the transmission and receipt of path names and other strings communicated between client and server.
3. Click **OK** to close the dialog box.
4. Click **Apply** to save the changes on EFT.

File Integrity Checking (XCRC)

Although TCP/IP checks that all packets are received, malformed packets or other mishaps can occur, leading the client to believe that a transfer was successful when it was not. EFT's file integrity command is defined as *XCRC*. Once an XCRC-enabled client (such as CuteFTP) performs a transfer, it can request EFT to do a checksum calculation on the file. If it matches the checksum on the client, then the transfer is deemed successful. Performing XCRC checksum calculations is processor intensive; enable or disable the feature accordingly.

XCRC applies to FTP and HTTP only, not SFTP. Refer to File Integrity Checking in FTP and SFTP below for details of file integrity checking in SFTP.

XCRC is a proprietary command and is not defined nor endorsed by any FTP-related RFC. Competing servers who want to implement this command may do so using the syntax described below.

```
XCRC <File Name>

XCRC <File Name>, <EP>

XCRC <File Name>, <SP>, <EP>
```

SP = Starting Point in bytes (from where to start CRC calculating)

EP = Ending Point in bytes (where to stop CRC calculating)

FTP Client Log Example

```
COMMAND:> XCRC "/Program Files/MSN Gaming
Zone/Windows/chkrzm.exe" 0 42575
```

- SP and EP are optional parameters. If not specified then it calculates the CRC for the whole file. If only EP is specified, then the CRC calculation starts from the beginning of the file to the EP.
- This command can be used for a single file at a time. It does not allow file lists as parameters.
- The standard CRC32 algorithm is used (for speed and efficiency).
- A client can invoke this command for uploads, downloads, and single and Multi-Part Transfers.

Server Reply	Indicates
`250 <XCRC>`	calculated CRC value
450 Requested file action not taken	file is busy
550 Requested action not taken	file is not found or has no read permission; or the SP or EP are not correct

File Integrity Checking in FTP and SFTP

FTP provides a very raw mechanism to transfer files – the data for a file is uploaded/downloaded as a stream of bits over a TCP/IP connection. There is no additional overhead on that operation, so it is fast; however, this also means that there are no intrinsic mechanisms for ensuring that the file got to the other end intact. That is why many servers, including EFT, support the XCRC command, an extension to the FTP protocol. The XCRC command performs a CRC32 checksum over the file (either the whole file, or a portion of the file if a byte range is specified on the command line). This gives a 32-bit value that EFT computes on the file, which can be compared to the 32-bit value computed on the client side. If both files are the same size and the CRC32 matches, then there is a very high probability that the files are identical and files were transferred correctly.

In contrast, SFTP ***does*** add overhead to the transfer of files. As a file is transferred between client and server, it is broken up into smaller chunks called "packets." For example, suppose each packet is 32KB. The SFTP protocol does a checksum on each 32KB file as it is sent, and includes that checksum along with that packet. The receiver gets that packet and decrypts the data, and then verifies the checksum. The checksum itself is "stronger" than the CRC32 checksum. (Because SFTP uses a 128-bit or higher checksum, such as MD5 or SHA, and because this is done on each and every packet, there is a very granular integrity checking that is accomplished as part of the transfer.) Thus, the protocol itself is slower (because of the additional overhead), but the successful completion of a transfer means, de facto, that it has be transferred integrally and there is no need for an additional check.

If you want to verify integrity, then use SFTP protocol and it is built-in or use FTP and after a transfer issue the raw command "XCRC /path/to/file" and read the results, comparing to a locally calculated CRC32 on the client side. EFT also supports querying the CRC32 value over the HTTP/S protocol by issuing a "HEAD" request to the file. The result of a HEAD method invocation on the HTTP/S engine will result in a response that includes the "X-CRC" header, which contains the CRC32 value of the file in question. This can be compared to the CRC32 computed over the local file, just like in the FTP case.

XCRC can be used on files larger than 2 GB.

To enable or disable the XCRC command

1. Open the **FTP Settings** dialog box.
2. Do one of the following:
   - To allow transfers, select the **Allow integrity checking (XCRC)** check box.
   - To block transfers, clear the **Allow integrity checking (XCRC)** check box.
3. Click **OK** to close the **FTP Settings** dialog box.
4. Click **Apply** to save the changes on the Server.

FTP Commands Supported by EFT

During FTP sessions, servers send and receive various numbered codes to/from FTP clients. Some codes represent errors; most others simply communicate the status of the connection.

When determining a course of action, review the entire log; some codes are informational only, others indicate that you have entered the wrong information, and others indicate what information you need to provide before continuing with your file transfer.

For brief explanations for the most common FTP status and error codes, refer to Knowledgebase article #10142 at https://kb.globalscape.com/KnowledgebaseArticle10142.aspx.

For a list of FTP commands supported by EFT, please refer to https://kb.globalscape.com/KnowledgebaseArticle10382.aspx.

Specifying a PASV IP or PASV Port Range

If EFT is behind a firewall or NAT device, you may need to specify EFT's IP address or range of ports used when issuing IP:PORT information to clients.

If you specify a PASV (passive) mode port range, you must open the same range of ports on your firewall.

To specify a PASV connection through a range of ports

1. Open the **FTP Settings** dialog box.
2. Select the **Assign PASV mode IP address** check box.
3. In the **IP** box, specify the Site's IP address as it should be seen by those outside of your network.

   This usually applies to SSL sessions when the NAT or firewall device cannot see nor properly map the internal IP address to connect to EFT. This also applies if the NAT or firewall device is misconfigured. You should first try connecting to EFT with this box left as is.

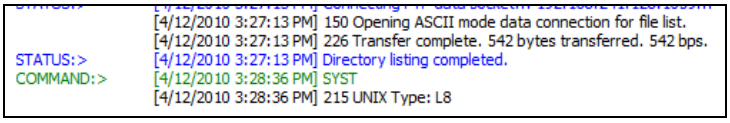
4. In the **Port Range** boxes, specify the range of ports EFT uses for PASV connections.

   Use this setting primarily to limit the amount of ports used for the data connection portion of the session, especially when the firewall or NAT device was configured to only allow traffic on certain ports.

5. Click **OK** to close the dialog box.
6. Click **Apply** to save the changes on EFT.

Specifying the Value Returned by the FTP SYST Command

A SYST request asks for information about the server's operating system. The server accepts this request with code 215. EFT, and most servers, respond with `215 UNIX Type: L8`:



Some clients disable essential features when they do not see particular strings in the SYST response. If your server requires a particular response, EFT provides an advanced property with which you can specify the value returned by the FTP SYST command. Refer to https://kb.globalscape.com/KnowledgebaseArticle10601.aspxfor details.

HTTP/S

(Requires the HTTP/S module) The Hypertext Transfer Protocol (HTTP) is an application layer protocol, designed within the framework of the Internet protocol suite, for distributed, collaborative, hypermedia information systems. HTTP functions as a request–response protocol in the client–server computing model. A web browser, for example, may be the client and EFT is the server. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body.

Hypertext Transfer Protocol Secure (HTTPS) is an extension of HTTP, used for secure communication over a network for authentication, privacy protection, and integrity of the transferred data while in transit. Unlike HTTP, HTTPS protects against man-in-the-middle attacks, and provides bidirectional encryption of communications between a client and server. HTTPS encrypts all message contents, including the HTTP headers and the request/response data.

The HTTP and HTTPS protocols can be enabled/configured on an EFT Site and inherited by the Settings Templates and user accounts. (You can then configure the Settings Templates and user accounts differently, if needed.) The topics below provide the procedures for configuring HTTP/S settings on Sites, Settings Templates, and user accounts.

- HTTP and HTTPS Overview
- Configuring HTTP or HTTPS Transfers
- Customizable HTTP Error Messages
- Enable HSTS
- Enabling User Access to the Web Transfer Client
- OCSP
- Redirecting HTTP to HTTPS
- Using WebDAV with EFT
- Invoke Web Service Action

HTTP and HTTPS Overview

If you specify HTTP for a Site created using the "strict security settings" option, EFT prompts you to disable insecure protocols, or continue with reason.

HTTP

HTTP is the communication protocol for establishing a connection with a Web server and transmitting HTML pages to the client browser or any other files required by an HTTP client application.

HTTP is often referred to as a "stateless" protocol. The connection is maintained between client and server only for the immediate request, after which the connection is subsequently closed. Each time you need something from EFT, your client (browser) makes a connection, gets that file, and then the connection is closed. Since you do not connect and stay connected, the browser remembers your username and password for you, so it can send the authentication hash along with every new connection request.

For example, when you type `http://www.globalscape.com/admin/whatsnew.aspx`in your browser's address bar and press ENTER, your browser uses HTTP as specified in the URL to send a command to EFT running at the host name www.globalscape.com with the HTTP command "`GET /admin/whatsnew.aspx HTTP/1.1`," and EFT replies with that file (the HTML that makes up the page). In that page, there are references to a number of files (for example, images, CSS documents, flash files), and your browser makes a separate connection to get each one of those resources.

How does HTTP support in EFT differ from a typical Web Server?

EFT is primarily a file transfer server, not a Web server. This means it is not meant to "serve up" Web pages such as a typical Web server does for connecting HTTP clients (such as your Web browser). However, there are provisions for transferring files in the HTTP protocol, which is a convenience when a connecting partner, customer, or employee does not have an FTP client installed, but does have an HTTP client or access to a Web page with HTTP PUT capabilities (usually an ActiveX control or Java applet).

When EFT is configured to allow HTTP file transfers, any HTTP client will be able to PUT (upload) or GET (download) files to EFT, provided the client supports both of these HTTP commands. Most Web browsers only support the GET command or, if they support the PUT command, they provide no interface for browsing to the user's local file system to select and upload (PUT) files onto EFT. A few dedicated clients (such as CuteFTP) and various thin clients (based on ActiveX controls or Java applets) support both PUT and GET capabilities, allowing these clients to transfer files to EFT in both directions.

For details of WebDAV and EFT, refer to Using WebDAV with EFT.

HTTP Limitations in EFT

- EFT allows you to customize messages sent by EFT upon connection, login, maximum connections reached, and disconnect (for FTP sessions). Due to the nature of the HTTP protocol, custom login messages are not displayed for connecting HTTP clients.
- Another limitation of HTTP is that after a connection is established, the browser sees EFT's root folder instead of the user's home holder. A workaround is to setup a distinct Site for HTTP sessions.
- Microsoft Internet Explorer browsers that have installed MS04-004 *Cumulative Security Update for Internet Explorer* (832894), no longer support URLs that contain username info, even though they are properly formed URLs. This problem is unique to Internet Explorer, and does not affect the other major browsers. For more information, refer to http://www.microsoft.com/technet/security/Bulletin/MS04-004.asp.
- If you create an Event Rule that sends a notification email for each successful login Event, an email is sent *every time* a user connected through HTTP changes directories. This is a result of HTTP being a stateless protocol and can result in a large volume of notification emails even when performing typical directory browsing.

HTTPS

HTTPS is the protocol for accessing a secure Web server when authentication and encrypted communication is possible. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The default TCP/IP port of HTTPS is 443. The session is then managed by a security protocol. HTTPS encrypts the session data using the SSL (Secure Socket Layer) protocol ensuring reasonable protection from eavesdroppers and man-in-the-middle attacks.

Secure Socket Layer (SSL) is a protocol for encrypting and decrypting data across a secure connection from a client to a server with SSL capabilities. EFT is responsible for

sending the client a certificate and a public key for encryption. If the client trusts EFT's certificate, an SSL connection can be established. All data passing from one side to the other will be encrypted. Only the client and EFT will be able to decrypt the data. The SSL protocol is the same protocol used in FTPS.

The following elements work together to establish a secure HTTPS connection:

- **Client**: The client must have SSL capabilities.
- **Certificate**: Certificates are digital identification documents that allow both servers and clients to authenticate each other. A certificate file has a **.crt** extension. Server certificates contain information about your company and the organization that issued the certificate (such as Verisign or Thawte) while client certificates contain information about the user and the organization that signed the certificate. You can choose to either trust or distrust a certificate. In some cases, the client's certificate must be signed by EFT's certificate to establish an SSL connection.
- **Session Key**: The client and EFT use the session key to encrypt data. It is created by the client via EFT’s public key.
- **Public Key**: The client encrypts a session key with EFT’s public key. It does not exist as a file, but is produced when a certificate and private key are created.
- **Private Key**: EFT's private key decrypts the client's session. The private key has a .key extension and is part of the public-private key pair.
- **Certificate Signing Request**: A Certificate Signing Request (CSR) is a PKCS10 request, which is an unsigned copy of your certificate. A certificate signing request is generated each time a certificate is created. A certificate signing request has a .csr extension. This file is used when you need to have your certificate signed. Once the Certificate Signing Request file is signed, a new certificate is made and can be used to replace the unsigned certificate.

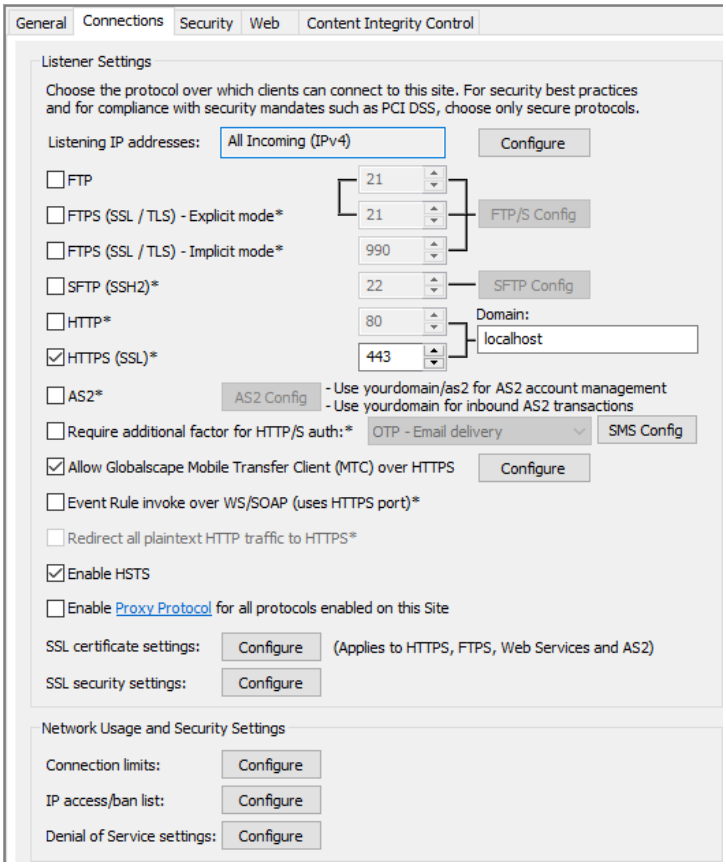
In Web pages that use HTTPS, the URL begins with **https** rather than **http**. HTTP clients should connect using standard requests (that is, https://domain_name). You can configure EFT to provide connecting clients with a certificate, and can require that the client provide a certificate upon connection (to validate the client's identity further).

Configuring HTTP or HTTPS Transfers

(Requires the HTTP/S module) You can enable or disable HTTP or HTTPS transfers for the Site, Settings Template, or user account on the **Connections**tab. (See also Configuring SSL on the Server.)

To enable HTTP or HTTPS transfers

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site, Settings Template, or user account that you want to configure.
3. In the right pane, click the **Connections**tab.



4. Select (enable) or clear (disable) the **HTTP**or **HTTPS (SSL)** check box, and then (if enabled):
    a. On the Site, specify the HTTP and HTTPS ports. The default port numbers are 80 and 443. (Note that Microsoft IIS also uses port 80 by default, so you will have to change one of them.)
    b. On the Site, specify whether to enable account management over HTTP/S and whether to redirect HTTP connections to HTTPS.

c. The Settings Template and/or user accounts will inherit the Site settings. If you want the Settings Template or user accounts to have a different setting than the Site, on the Settings Template and/or user account **Connections**tab, select (enable) or clear (disable) the **HTTP**or **HTTPS** check box.

5. Click **Apply**to save the changes on EFT. If you are enabling HTTPS, you must also assign an SSL certificate.

Related Topics

- Redirecting HTTP to HTTPS
- Enabling the Account-Management Page
- Enabling User Access to the Web Transfer Client
- SSL

Customizable HTTP Error Messages

(Requires the HTTP/S) During your HTTP sessions, you will receive various numbered codes from Web servers. Some codes represent errors; most others simply communicate the status of the connection. For brief explanations for the most common status and error codes, refer to Knowledgebase article #10141 at https://kb.globalscape.com/KnowledgebaseArticle10141.aspx.

EFT provides customizable HTTP error messages in HTML files in the **\HTTPMessages** folder (for example, **C:\ProgramData\Globalscape\EFT Server\HTTPMessages**).

Each time the EFT service starts up, each of the HTTPMessages files is created if they do not already exist. When an HTTP response is needed, EFT first tries to load the response from files in this location. Failing that, EFT uses its internal response strings.

HTTP responses that are stored through this mechanism that can be customized are limited to the following responses:

HTTP Error	Default Text
BAD_PARAMETER	HTTP/1.1 406 Bad Parameter; The requested URL was not found on this server.
BAD_REQUEST	HTTP/1.1 400 Bad Request
BAD_URI	Bad URI
FORBIDDEN	HTTP/1.1 403 Forbidden
INTERNAL_SERVER_ ERROR	HTTP/1.1 500 Internal Server Error
MAX_QUOTA_REACHED	HTTP/1.1 413 Max Quota Reached
NOT_FOUND	HTTP/1.1 404 Object Not Found; The requested URL was not found on this server.
NOT_IMPLEMENTED	HTTP/1.1 501 Not Implemented
PRECONDITION_FAILED	HTTP/1.1 412 Precondition Failed
REQUEST_TOO_LARGE	HTTP/1.1 413 Request Entity Too Large
SERVICE_UNAVAILABLE	HTTP/1.1 503 Service Unavailable
URI_TOO_LARGE	HTTP/1.1 414 Request-URI Too Large

Enable HSTS

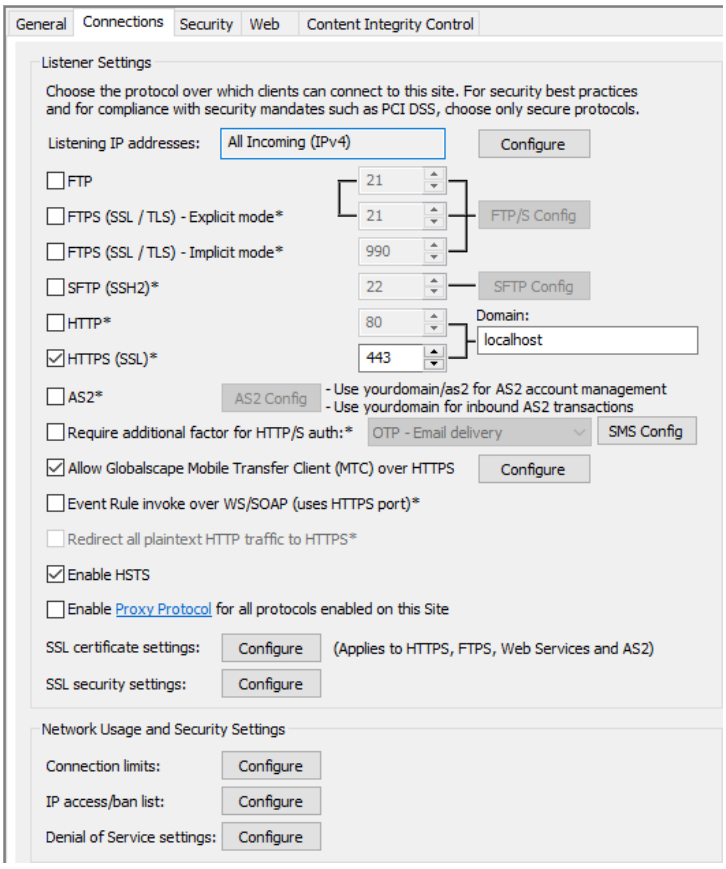
HTTP Strict Transport Security (HSTS) is web security policy to protect websites against protocol downgrade attacks and cookie highjacking. You can use HSTS response headers to tell browsers that your site only works via HTTPS. The response header indicates to the browser that you don't want to use HTTP requests, and it will automatically make requests to the same origin with a secured connection. When you try to access the same URL via HTTP again, browsers will use HTTPS and redirect internally.

- HSTS can be enabled in the administration interface without "HTTP -> HTTPS redirect" enabled.
- HSTS is available only when HTTPS is enabled.
- EFT sends HSTS headers when the client connects (if HSTS is enabled).
- HSTS is enabled by default on new installs when HTTPS is enabled.
- HSTS is enabled by default on upgrades if HTTPS was enabled before the upgrade.
- HSTS is part of the HTTP/S module.

> **NOTE:** A more granular way of defining which resources and actions are allowed on your website is to define a Content Security Policy (CSP) header. For more about CSP, refer to Knowlegebase article 11435 - Specify CSP.

To enable HSTS

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Connections**tab.



4. Select the **Enable HSTS** check box.
5. Click **Apply**to save the changes on EFT.

User Access to the Web Transfer Client

(Requires the HTTP/S module) Before users can log in to EFT using the Web Transfer Client (WTC), EFT administrator must configure EFT to allow connections from the WTC. Active Directory domain users must have logon permission on EFT computer in order to log on to EFT through the WTC. This is accomplished by adding AD domain users to the "Allow log on locally" list on EFT computer. If an AD domain user is not in this list, logging on to EFT through the WTC will fail and an error message appears informing the user that Local login access is required to log on to EFT.

Setting Defaults

The admin-configuration.jsonfile is used to set defaults for all the WTC settings, providing better control over the end-user experience, such as upload limit, permissions, participant limit, and others. The file can be opened and edited in a text editor and is stored in the ..**\Web**directory. (The **\Web** directory is in the cluster share for HA installations.)

In v8.0.4 and earlier: **Web\public\EFTClient\shadowfax\wtc\assets**

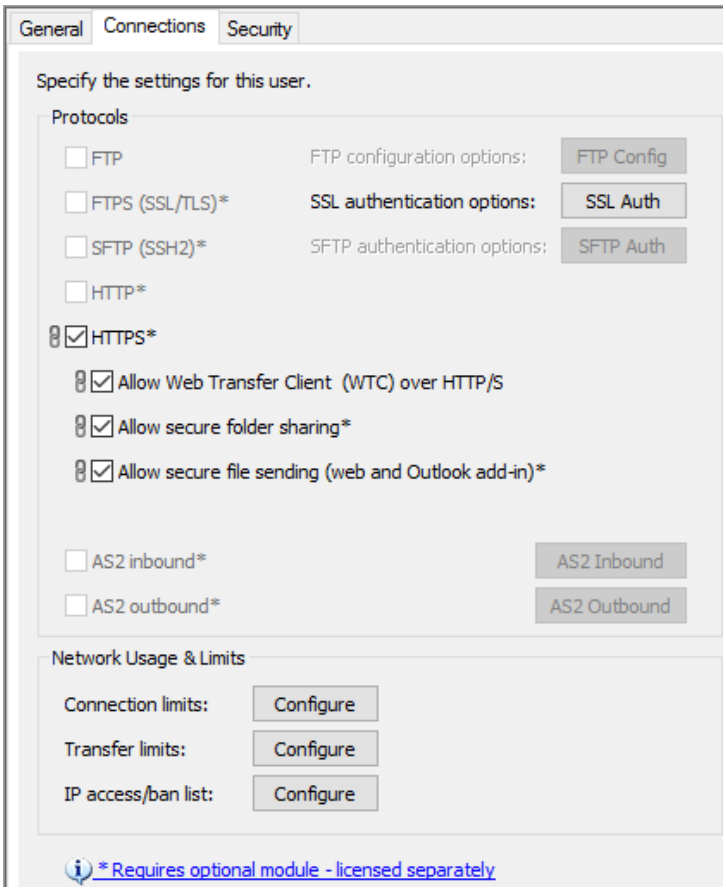
In v8.0.5 and later: **\Web\Shadowfax\portal\assets**

Refer also to Enable Multifactor Authentication for Workspaces

Stopping and restarting the Site disconnects everybody who is connected; users must log back in.

To configure EFT to allow Web Transfer Client Connections

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Settings Template or user account.
3. In the right pane, click the **Connections**tab.



4. In the **Protocols** area, select the **Allow Web Transfer Client over HTTP/S** check box.

   HTTPS must also be enabled.

5. Click **Apply**.

Online Certificate Status Protocol (OCSP)

(Requires the HTTP/S module) When you go to a website that uses an SSL certificate, such as a bank or shopping site, the browser needs to verify that the website is using a valid (current) SSL certificate. The Online Certificate Status Protocol (OCSP) is used to verify whether an X509 SSL certificate is still valid.

When verifying the security of a new HTTPS connection, it is up to the connecting client (for example, web browser) to verify that a certificate presented by an SSL server (that is, EFT) has not been revoked by the CA that issued the certificate. To verify whether the certificate is valid, the browser queries an OCSP server, such as a certificate authority (CA).

Traditionally, the client (web browser) performs the SSL handshake to obtain the server certificate, then it performs queries against Certificate Revocation Lists (CRLs) and Online Certificate Status Request Protocol (OCSP) servers. This causes some extra traffic and cryptographic operations to take place during the initial connection to a remote HTTPS server, which causes a perceptible delay in that connection.

OCSP Stapling

"OCSP stapling" allows the web server to query the OCSP server and then save the response, which is then delivered to the browser, and is valid for a certain period of time. With OCSP stapling, the CA no longer receives the revocation requests directly from the browser, and there is no need for a separate network connection to the CA, preventing negotiation delays. A token is passed to the client in place of the client having to go ask for the full list/parse on each connect. OCSP Stapling is an optimization mechanism that allows all the verification of the server certificate to happen within the initial SSL handshake, rather than requiring additional round trips to other servers.

Without the stapled OCSP certificate being presented by the HTTPS server, it is the responsibility of the connecting client (for example, web browser) to use traditional OCSP or CRL queries to CAs to obtain revocation information. Both mechanisms are still available, and initiated by the client, not the server.

Thus, the absence of OCSP stapling support is not a security vulnerability, but a lack of optimization. Browsers will still validate server identity via the SSL certificate and any revocation information from CA sources.

If you have F5 Big IP LTM devices (LTM 11.6 or later), you could configure them to terminate SSL connections at that device, which means that you could easily add OCSP Stapling to your certificates using the traffic manager. Traffic would then be forwarded along as HTTP to the server. (The F5 Big IP LTM needs to have an iRule to add an "X-ORIGINAL-PROTOCOL" header to all HTTP requests.)

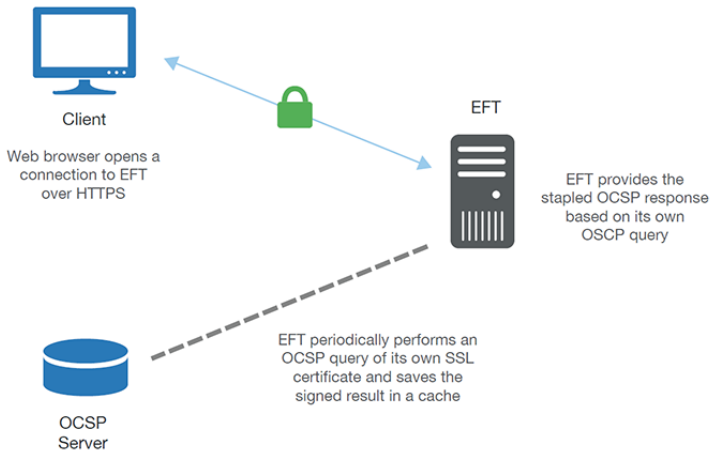
Refer to https://lessonsintech.wordpress.com/2016/02/10/configure-ocsp-stapling-f5-ltm/and https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ssl-administration-11-6-0/4.htmlfor more information.

OCSP Stapling in EFT

1. The web browser opens a connection to EFT over HTTPS. Part of the handshake includes an extension request that asks for the stapled OCSP response.
2. EFT, if it already has that response, simply returns the response to the client.

3. EFT periodically performs an OCSP query of its own SSL certificate, in case there have been any revocations or changes, and then saves the signed result into a cache. It is from there that EFT will offer the stapled OCSP response to the web browser. The round-trip between EFT and the OCSP server does *not* happen for every browser request, but only when the OCSP response is not found in the EFT cache, or if the cached response has expired.

The graphic below illustrates the process of OCSP stapling in EFT at a very high level.



How can I verify that OCSP stapling in EFT is working?

Because the SSL handshake itself is doing the OCSP Stapling request and response, you should be able to verify that stapling works for any protocol endpoint (FTPS and HTTPS and AS2) by using the OpenSSL command-line client, and passing in the "-status" flag, which indicates that the client *hello* needs to request the certificate status request (that is, "ocsp stapling request"):

```
openssl s_client -status -no_ssl2 -no_ssl3 -no_tls1  -host
 eft.company.com -port 443
```

You can observe the output from OpenSSL (and/or look at Wireshark captures) to see if the OCSP request and response are as expected. (Once you get past the handshake and establish SSL tunnel, the rest of the protocol doesn't really matter.)

OCSP Stapling in EFT does not support proxy configurations.

Refer to the Knowledgebase for OCSP-related advanced properties:

- https://kb.globalscape.com/KnowledgebaseArticle11362.aspxAdjust for time drift (skew) between the CA and EFT for OCSP requests

- https://kb.globalscape.com/KnowledgebaseArticle11363.aspxSpecify a maximum allowable age for OCSP stapling responses
- https://kb.globalscape.com/KnowledgebaseArticle11364.aspxOverride the OCSP responder URI specified in the certificate's AIA extension
- https://kb.globalscape.com/KnowledgebaseArticle11365.aspxEnable the OCSP response
- https://kb.globalscape.com/KnowledgebaseArticle11366.aspxOCSP Stapling cache timeout

Redirecting HTTP to HTTPS

(Requires the HTTP/S module; redirect not available in Product Name) EFT allow you to redirect all HTTP connections to HTTPS in the administration interface.

When HTTPS is enabled, EFT will automatically redirect HTTP traffic to HTTPS for logins, forced password changes, and lost username and password functionality. An advanced property can be used to prevent this redirect. The redirect check box described below controls both the login page and the connection, but only when HTTPS is enabled. The registry override's main purpose is to control whether the logon portion of the session is redirected to HTTPS when redirect is OFF in the administration interface. (The redirect check box is unavailable when HTTPS is disabled.)

If you have configured HTTPS transfers on the Site, you can redirect HTTP to HTTPS at the Site level. Doing so disables HTTP transfers.

EFT simply tells the connecting client that the resource was moved to the new HTTPS URL. The connecting client decides whether it will allow the redirect, because the new URL could be on a different server.

In general, the redirect process includes the following steps:

1. Client sends a request to the HTTP port (by default, port 80).
2. EFT redirects all plain HTTP requests to HTTPS (by default, port 80 to port 433). EFT replies to the client with 302 code (the requested resource resides temporarily under a different URL), and sends the client the new URL where the resource is now located.
3. The client now knows that the resource is not available at the old URL and knows the new URL. Client decides whether it wants to connect to the new URL and get this resource.

Refer to RFC 2616, section 10, http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html, for more information about redirection on HTTP.

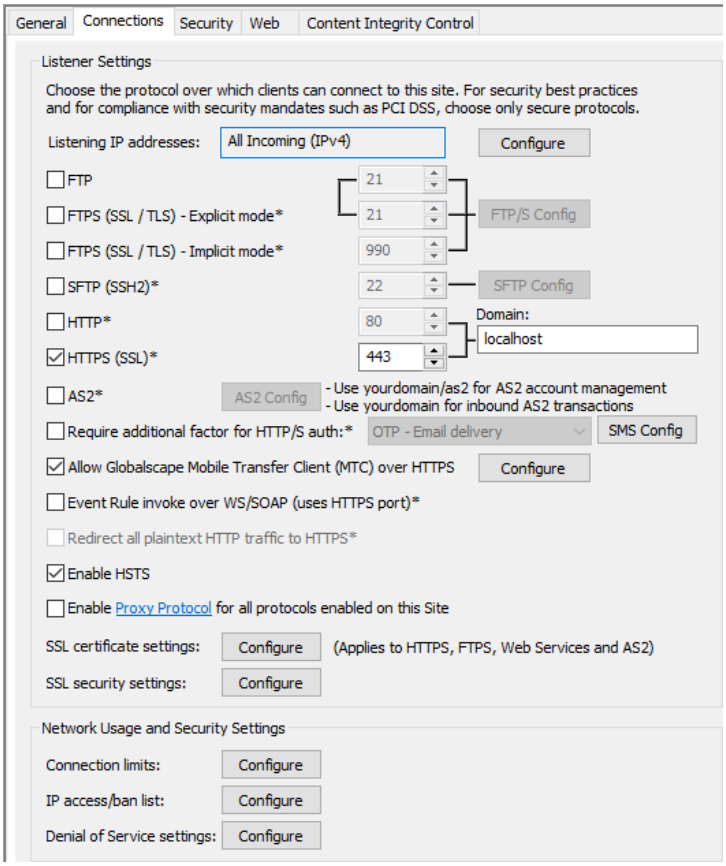
The redirect option also affects incoming AS2 requests through HTTP. If the connecting AS2 client does not allow redirection to a different port, the connection will fail.

If the redirect is not enabled, logins to WTC will still go to HTTPS, but then revert to HTTP after login.

To redirect HTTP to HTTPS

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site you want to configure.

3. In the right pane, click the **Connections**tab.



4. Select the **HTTPS (SSL)** check box and configure SSL if not already configured.
5. Select the **Redirect all plaintext HTTP traffic to HTTPS** check box.
6. Click **Apply**to save the changes on EFT.

Even if **HTTP**is enabled for the user or Settings Template, HTTP transfers will be redirected to the HTTPS port (443 by default).

EFT Web Service

The Web Service allows administrators to initiate EFT workflow from an external application such as an enterprise scheduler. The WebService interface follows the model of ASP.NET Web services, providing a page for the services definition document (WSDL) and an HTML form that can be used to test available service methods. (Download and use the Web Service scripts to test the Web Service with Powershell.)

The procedures below provide instructions to:

Enable the Web Service in EFT

Use the Invoke Web Service Action

- Access to Web Service requires authentication with a COM-enabled Server administrator account; without proper authentication and COM privileges, EFT returns a `401 Unauthorized HTTP error` to the requestor.
- An SSL certificate is required to use Web Service, because EFT sends the HTTP Web Services requests via HTTPS. (Specify SSL versions and ciphers before enabling SSL connections. SSL must first be enabled on EFT and the Site.)
- The Web Service is enabled in the Site's **Listener Settings** area. EFT allows you to turn on Web Service without selecting the **HTTPS**check box, but it checks for an SSL certificate, because it will automatically redirect HTTP to HTTPS. Even when the **HTTPS** check box is not selected, Web Service requests are handled by the HTTPS engine (port 443 listener, by default), but other HTTPS requests will still get the 503 Service unavailable response.
- EFT uses a template for the WSDL to construct the final WSDL. External tools can use the WSDL by pointing to the URL that deploys the WSDL file at
- **http://localhost/WebService/InvokeEventRule?wsdl**, where "localhost" is the IP address, computer name, or DNS name that points to the EFT service that is hosting the web service.
- Requests to any /WebService URL is logged to the text log and ARM system just as any other HTTP request.
- The Web Service timeout is set to 60 seconds. You can change the timeout value with the advanced property described in https://kb.globalscape.com/KnowledgebaseArticle10553.aspx.

Requests to any **/WebService**URL are logged to the text log and ARM database just as any other HTTP request. A request that does not match the **/WebService/InvokeEventRule**URL or that does not include the required parameters, results in a `400 Bad Request HTTP error`.

The **/WebService** page displays a list of Web services available with EFT. This page is generated from an HTML page in EFT installation folder, in a subfolder called **WebService**.

By default, the following files are installed in: **C:\Program Files\Globalscape\EFT Server\Web\WebServices**

- **\EFTWebServices_MAIN.html**- Used to define the Web Services landing page; provides a link to **InvokeEventRule.html**.
- **\InvokeEventRule\EFTWebServices_InvokeEventRule.html**- Used to define the Web interface from which you can remotely invoke Event Rules on EFT.
- **\InvokeEventRule\EFTWebServices.wsdl**- Web Services Description Language (WSDL) configuration file. (For details of how WSDL files are used, refer to the World Wide Web Consortium documentation at http://www.w3.org/TR/wsdl.)

How EFT Supports the Web Service

EFT supports both POST and GET HTTP requests to "/WebService/InvokeEventRule" with two parameters "EventRuleName" and "EventParams" and triggers an Event Rule that is specified in the "EventName." The Web Service supports the REST invocation model, supporting both POST and GET methods for invocation.

1. If an input is missing any of "EventRuleName" or "EventParams" it returns an HTTP 400 error.
2. If both "EventRuleName" and "EventParams" are presented but:
    a. "EventRuleName" is wrong (no Event Rule exists with such name), it returns .xml with result code of -1.
    b. "EventParams" are incorrect (wrong variable names, too many, too few), EFT looks for Rule variables in the input and replaces those values with found ones. All additional variables are ignored. If a Rule variable is not found in URL then it will be set to "N/A." The result code in .xml will be the Event execution result code.

HTTP GET

The following is a sample HTTP GET request and response. Replace the placeholders with values.

```
GET /WebService/InvokeEventRule?EventRuleName=string&
EventParams=string HTTP/1.1 Host: localhost

HTTP/1.1 200 OK Content-Type: text/xml; charset=utf-8
```

```
Content-Length: length <?xml version="1.0" encoding="utf-8"?>
<int xmlns="http://mydomain/">int<int>
```

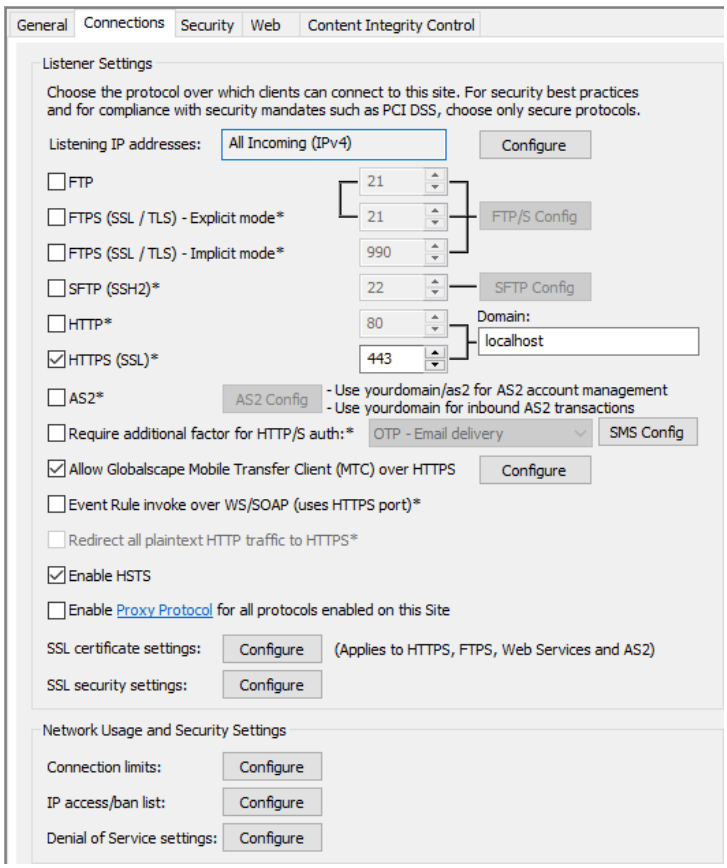
HTTP POST

The following is a sample HTTP POST request and response. Replace the placeholders with values.

```
POST /WebService/InvokeEventRule HTTP/1.1 Host: localhost
Content-Type: application/x-www-form-urlencoded Content-Length:
length EventRuleName=string&EventParams=string

HTTP/1.1 200 OK Content-Type: text/xml; charset=utf-8
Content-Length: length <?xml version="1.0" encoding="utf-8"?>
<int xmlns="http://mudomain/ ">int</int>
```

To enable the Web service in EFT

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site that you want to configure.
3. In the right pane, click the **Connections** tab.



4. Select the **Event Rule invoke over WS/SOAP (uses HTTPS port)** check box.

   IMPORTANT: If this is not enabled, you will not be able to log in to the Web Service.

5. Click **Apply** to save the changes on EFT.

To use the scripts for testing Web Service

Use one of the attached scripts to test Web Service (copy into PowerShell).

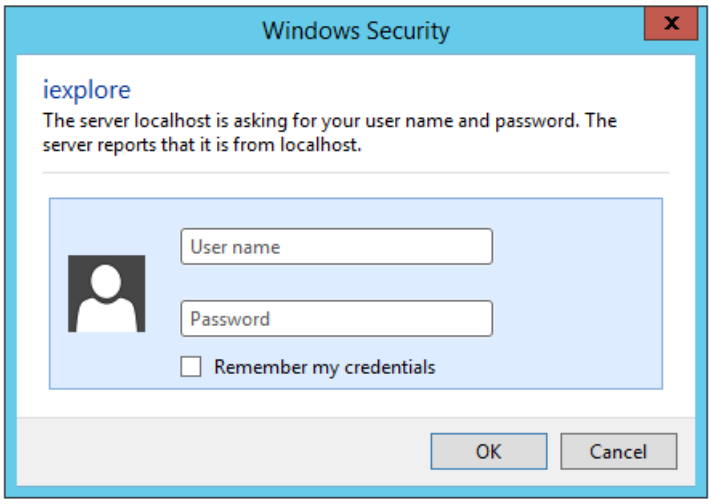
- **EFT.InvokeEventRule.ps1** uses regular output -1, 0 or 1 (classic SOAP)
  - Change the various strings at the top for host, administrator username, password, and event rule name.
- **InvokeEventRule.ps1** returns all context variables from the rule (behaves a bit more REST like, even though the response is XML, not json).
  - Add the advanced property "EventWebServiceResponseAddContextVariables" to the AdvancedProperties.JSON file. You must set this property to get the payload from EFT in response showing the context variables.
  - Change the administrator username and password various strings at the top of the script.
  - Modify the Invoke-WebRequest method, including the host, event rule name, and optional parameters.

To execute an Event Rule using Web Service

1. Open a browser and navigate to EFT URL appended with `/WebService`. The **WebService** page appears.

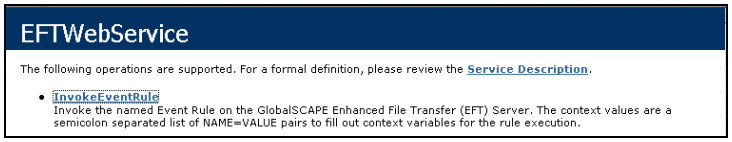
   IMPORTANT: You must change the URL of the Site and the port number if you are not using "localhost" and port 443, as shown below!

2. A login prompt appears. Provide a COM-enabled Server administrator account login credentials. If the **Event Rule invoke over WS/SOAP (uses HTTPS port)** check box is not enabled on the Connections tab of the Site, you will not be able to log in to the Web Service.

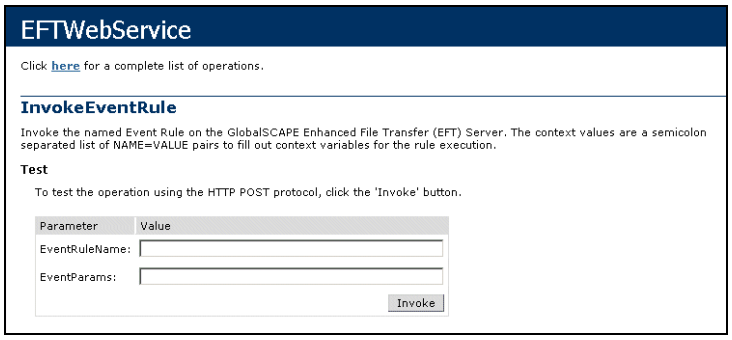


IMPORTANT: EFT leverages the USER https port (443 by default); however, WebService uses the Server administrator accountlogin credentials, not USER credentials!

3. The EFTWebService interface appears.



4. Click **InvokeEventRule.**Another Web page, **/WebService/InvokeEventRule**, displays a form for invoking an Event Rule.



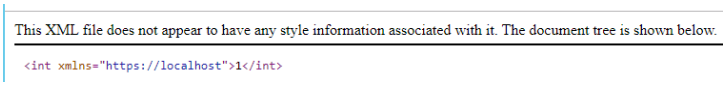
5. In the **EventRuleName**box, type the name of the Event Rule.
6. In the **EventParams**box, type one or more variables, separated by semicolons.
7. Click **Invoke**. The Event Rule is executed.

   All WebService responses use the Site's domain name as the namespace for the WebService.

   For example, in the **EventRuleNameValue** box, type `Backup and Cleanup`. Leave **EventParams**blank, and then click **Invoke**. The browser returns the following string:

```
<int xmlns="HTTPS://localhost:443/">1</int>
```

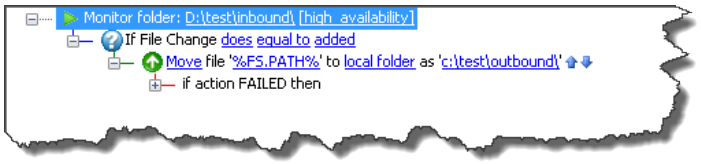
- 0 indicates failure
- 1 indicates success
- -1 indicates EFT could not find the Event Rule (for example, the requested EventName does not exist or was not typed correctly.)

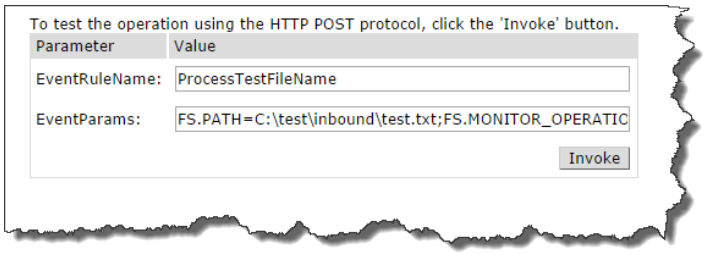


For this example, you can open the /**Backup/**folder and see that a backup file was created (for example, **C:\ProgramData\Globalscape\EFT Server\Backup**).

Using Web Service Examples

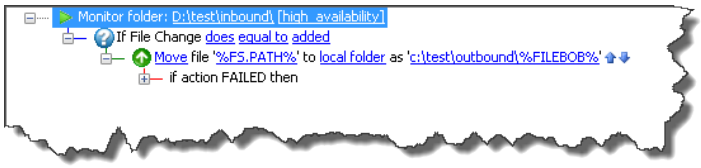
Folder Monitor






```
EventParams=FS.PATH=C:\test\inbound\test.txt;FS.MONITOR_
OPERATION=added
```

As you can see, the FS.MONITOR_OPERATION is part of the Condition and must be passed along with the variable of choice; in this case it is FS.PATH or any other variable that is created.




```
EventParams=FS.PATH=C:\test\inbound\test.txt;FS.MONITOR_
OPERATION=added;FILEBOB=test.filebob.txt
```

As you can see above, the variable is a custom variable applied to this event rule, outside of the EFT variables.

Timer Event

EventParams=FILEBOB=test.filebob.txt

The Timer Event is the least used Event Rule in EFT to download files, move them, or to automate an Advanced Workflow Script/custom command. Using the Web Services allows you to manipulate custom variables for the specific environment or file that needs to be processed. In the case above, the Timer event is being used as a transmission only, triggered by a remote process using “wget”.

Passing the URL to WebServices

As the HTTP GET states:

```
GET
/WebService/InvokeEventRule?EventRuleName=string&EventParams=str
ing
 HTTP/1.1
```

Based on this information, the URL should contain the following:

- **EventRuleName**=ProcessTestFileName
- **EventParams**=FS.PATH=C:\test\inbound\test.txt;
- **FS.MONITOR_OPERATION**=added

Combine the parameters:

```
http://localhost/WebService/InvokeEventRule?EventRuleName=Proces
sTestFileName&EventParams=FS.PATH=C:\test\inbound\test.txt;FS.MO
NITOR_OPERATION=added
```

> **NOTE:** The ampersand “&” is used to separate the **EventRuleName**and **EventParams**, but you will use the semi-colon (;) to separate more than 1 **EventParams**that is required to make the Event Rule work correctly.

Using WebDAV in EFT

EFT supports a subset of the WebDAV, which is an extension to the HTTP/1.1 protocol that allows clients to perform remote Web content authoring operations. HTTP defines many headers that can be used in WebDAV requests and responses. WebDAV provides functionality to create, change, and move documents on a remote server (typically a web server or "web share"). This is useful, among other things, for authoring the documents that a web server serves, but can also be used for general web-based file storage that can be accessed from anywhere. Important features in WebDAV protocol include locking (overwrite prevention), properties (creation, removal, and querying of information about author, modified date, etc.), name space management (ability to copy and move Web pages within a server's namespace), and collections (creation, removal, and listing of resources). Refer to the HTTP Extensions for Web Distributed Authoring and Versioning standard for more information.

As of EFT v8.0.5, the MKCOL method is no longer supported "out of the box"; however, you can enable it in the **admin-configuration.json** file. A new advanced property has been added to the file, `"tunnelNonHttpVerbs": false`. If NOT present (default) or set to `false`, it means WTC will continue to use MKCOL, COPY, and so on; if present and set to `true`, WTC will use POST with X-HTTP-Method-Override header for tunneling non-standard HTTP verbs.

When **DisableMKCOLRequest** is true, EFT enables incoming MKCOL requests. (Added in v8.2)

All methods\headers marked as supported below (MKCOL, GET for Collections, DELETE for Collections, PUT for Non-Collection Resources, MOVE + Destination header) are used by ClientFTP and Web Transfer Client. EFT's Advanced Workflows work with the WebDAV protocol in the Get Email Action, Send email Action, and Exchange Action.

The table below indicates which WebDAV extensions are supported by EFT. The numbers indicate the section of the standard. Descriptions, status codes, and examples from the standard appear after the table.

Method	EFT Support
9.1. PROPFIND Method	NOT supported
9.2. PROPPATCH Method	NOT supported
9.3. MKCOL Method	Supported
9.4. GET, HEAD for Collections	Supported
9.5. POST for Collections	NOT Supported
9.6.1. DELETE for Collections	Supported
9.7.1. PUT for Non-Collection Resources	Supported

Method	EFT Support
9.7.2. PUT for Collections	NOT supported
9.8. COPY Method	NOT supported
9.9.1. MOVE for Properties	NOT Supported
9.9.2. MOVE for Collections	Supported
9.9.3. MOVE and the Overwrite Header	NOT Supported
9.10. LOCK Method	NOT Supported
9.11. UNLOCK Method	NOT Supported
10. HTTP Headers for Distributed Authoring	NOT Supported
10.1. DAV Header	NOT Supported
10.2. Depth Header	NOT Supported
10.3. Destination Header	Supported
10.4. If Header	NOT Supported
10.5. Lock-Token Header	NOT Supported
10.6. Overwrite Header	NOT Supported
10.7. Timeout Request Header	NOT Supported

Descriptions, Examples, and Error Codes

Method	Description, Examples, and Error Codes

9.3. MKCOL Method	MKCOL creates a new collection resource at the location specified by the Request-URI.
	
	Example:
	
	`>>Request`
	
	`MKCOL /webdisc/xfiles/ HTTP/1.1`
	
	`Host: www.example.com`
	
	`>>Response`
	
	`HTTP/1.1 201 Created`
	
	Status and error codes:
	• **201** (Created) - The collection was created.
	• **403** (Forbidden) - This indicates at least one of two conditions: 1) the server does not allow the creation of collections at the given location in its URL namespace, or 2) the parent collection of the Request-URI exists but cannot accept members.

Method	Description, Examples, and Error Codes
9.4. GET, HEAD for Collections	The semantics of GET are unchanged when applied to a collection, since GET is defined as, "retrieve whatever information (in the form of an entity) is identified by the Request-URI" [RFC2616]. GET, when applied to a collection, may return the contents of an "index.html" resource, a human-readable view of the contents of the collection, or something else altogether. Hence, it is possible that the result of a GET on a collection will bear no correlation to the membership of the collection.
9.5. POST for Collections	Since by definition the actual function performed by POST is determined by the server and often depends on the particular resource, the behavior of POST when applied to collections cannot be meaningfully modified because it is largely undefined. Thus, the semantics of POST are unmodified when applied to a collection.

9.6.1. DELETE for Collections	DELETE instructs that the collection specified in the Request-URI and all resources identified by its internal member URLs are to be deleted.
	
	`>>Request`
	
	`DELETE /container/ HTTP/1.1`
	
	`Host: www.example.com`

9.7.1. PUT for Non-Collection Resources	A PUT performed on an existing resource replaces the GET response entity of the resource.
9.9.2. MOVE for Collections	A MOVE with "Depth: infinity" instructs that the collection identified by the Request-URI be moved to the address specified in the Destination header, and all resources identified by its internal member URLs are to be moved to locations relative to it, recursively through all levels of the collection hierarchy.

10.3. Destination Header	The Destination request header specifies the URI that identifies a destination resource for methods such as COPY and MOVE, which take two URIs as parameters.
	
	`Destination = "Destination" ":"`
	`Simple-ref`

SFTP

The SSH File Transfer Protocol (SFTP) is a network protocol that provides file access, file transfer, and file management over any reliable data stream. It was designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH) version 2.0 to provide secure file transfer capabilities. The IETF Internet Draft states that, even though this protocol is described in the context of the SSH-2 protocol, it could be used in a number of different applications, such as secure file transfer over Transport Layer Security (TLS) and transfer of management information in VPN applications.

The SFTP/SSH protocol can be enabled/configured on an EFT Site and inherited by the Settings Templates and user accounts. The setting is inherited by the Settings Templates and user accounts, but you can configure them differently, if needed.

- SFTP Advanced Properties
- SFTP Logging
- SFTP Encryption Algorithms
- Creating an SSH Key Pair
- Configuring SFTP for a Site
- Configuring User SFTP Authentication
- Managing SFTP Keys for the Site
- Encoding for SFTP Transfers
- Extracting the Public SFTP Key
- Modifying the SFTP Identification String
- SFTP FIPS
- SFTP Key Support
- Specifying SFTP Algorithms
- SSH Key Formats
- Using SFTP (SSH) with Radius/RSA SecurID
- Viewing or Modifying MAC Settings

SFTP Outgoing Ciphers and Advanced Properties

Advanced Propertiesare available for enabling or disabling the following SFTP properties. For the most part, the advanced property is used to turn OFF a specific cipher for outbound that is allowed for inbound; however, in some instances, due to the security risk involved, the advanced property must enable that algorithm, *even if it is already enabled for inbound connections via the interface.*

Outgoing Ciphers

Enabled by default:

- aes256-gcm@openssh.com (can be disabled for client outbound via Advanced Property SFTP2_AES256_GCM_AT_OPENSSH_COM to false)
- aes256-ctr (can be disabled for client outbound via Advanced Property SFTP2_AES256CTR to false)
- aes256-cbc (can be disabled for client outbound via Advanced Property SFTP2_AES256 to false)
- rijndael-cbc@lysator.liu.se (can be disabled for client outbound via Advanced Property SFTP2_RIJNDAEL_CBC_AT_LYSATOR_LIU_SE to false)
- aes192-ctr (can be disabled for client outbound via Advanced Property SFTP2_AES192CTR to false)
- aes192-cbc (can be disabled for client outbound via Advanced Property SFTP2_AES192 to false)
- aes128-gcm@openssh.com (can be disabled for client outbound via Advanced Property SFTP2_AES128_GCM_AT_OPENSSH_COM to false)
- aes128-ctr (can be disabled for client outbound via Advanced Property SFTP2_AES128CTR to false)
- aes128-cbc (can be disabled for client outbound via Advanced Property SFTP2_AES128 to false)
- 3des-cbc (can be disabled for client outbound via Advanced Property SFTP2_TripleDES to false)
- chacha20-poly1305@openssh.com (can be disabled for client outbound via Advanced Property SFTP2_CHACHA20_POLY1305_AT_OPENSSH_COM to false)

Disabled by default:

- cast128-cbc (can be enabled for client outbound via Advanced Property SFTP2_CAST128 to true)

- blowfish-cbc (can be enabled for client outbound via Advanced Property SFTP2_Blowfish to true)
- arcfour (can be enabled for client outbound via Advanced Property SFTP2_ ARCFOUR to true)

Advanced Properties related to SFTP:

- EnableXferLog - (enable transfer logs) Set to true to improve log performance
- CloseFinishedItemLog - (enable removal of successful logs) Set to true to improve log performance
- SFTP2_Log - Set to 1 to enable ClientFTP SFTP logging.
- SFTP2_Log_Level - ClientFTP SFTP log level.
- SFTP2_AuthByKey - Enable ClientFTP SFTP authentication by key.
- SFTP2_AuthByPassword - Enable ClientFTP SFTP authentication by password.
- SFTP2_UseCompression - Enable ClientFTP SFTP compression.
- SFTP2PrivateKey - ClientFTP SFTP private key.
- SFTP2PublicKey - ClientFTP SFTP public key.
- SFTPDiscardClientTimestamp - Disregard client initiated SFTP SSH_FXP_ FSETSTAT and SSH_FXP_SETSTAT command to change the date/timestamp of files.
- SFTPEnableGroup1Kex - Enable or disable diffie-hellman-group1-sha1 KEX for SFTP
- SFTPEnableGroupsExchangeKex - Enable or disable diffie-hellman-group-exchange-sha1 and diffie-hellman-group-exchange-sha256 KEXes for SFTP
- SFTPOutQueueBytesLimit - Specifies (in bytes) upper limit of SFTP out queue. 0 - no limit
- SFTP2_AES128 - Setting to 1 enables the AES128 cipher algorithm.
- SFTP2_AES128CTR - Setting to 1 enables the AES128CTR cipher algorithm.
- SFTP2_AES256 - Setting to 1 enables the AES256 cipher algorithm.
- SFTP2_AES256CTR - Setting to 1 enables the AES256CTR cipher algorithm.
- SFTP2_ARCFOUR - Setting to 1 enables the ARCFOUR cipher algorithm.
- SFTP2_Blowfish - Setting to 1 enables the Blowfish cipher algorithm.
- SFTP2_CAST128 - Setting to 1 enables the CAST128 cipher algorithm.
- SFTP2_MD5 - Setting to 1 enables the MD5 MAC algorithm.
- SFTP2_MD5_96 - Setting to 1 enables the MD5_96 MAC algorithm.
- SFTP2_SHA1 - Setting to 1 enables the SHA1 MAC algorithm.
- SFTP2_SHA1_96 - Setting to 1 enables the SHA1_96 MAC algorithm.

- SFTP2_SHA2_256 - Setting to 1 enables the SHA2_256 MAC algorithm.
- SFTP2_SHA2_512 - Setting to 1 enables the SHA2_512 MAC algorithm.
- SFTP2_TripleDES - Setting to 1 enables the TripleDES cipher algorithm.
- SFTP2_Twofish - Setting to 1 enables the Twofish cipher algorithm.
- SFTP2_TWOFISH128 - Setting to 1 enables the TWOFISH128 cipher algorithm.
- SFTP2_TWOFISH256 - Setting to 1 enables the TWOFISH256 cipher algorithm.
- SftpClientCiphers - Override client's enabled Ciphers and their order. Example: "SftpClientCiphers": "aes128-ctr,aes192-ctr,aes256-ctr" The combined values should be comma separated *without* any additional characters. (If not set, then it uses default ordering which is same as server inbound order.)
    - For non-FIPS, SftpClientCiphers, you can combine values:
        - aes256-gcm@openssh.com
        - aes256-ctr
        - aes256-cbc
        - rijndael-cbc@lysator.liu.se
        - twofish256-cbc
        - twofish-cbc
        - aes192-ctr
        - aes192-cbc
        - aes128-gcm@openssh.com
        - aes128-ctr
        - aes128-cbc
        - twofish128-cbc
        - 3des-cbc
        - chacha20-poly1305@openssh.com
        - cast128-cbc
        - blowfish-cbc
        - arcfour
    - For FIPS, SftpClientCiphers AP you can combine values
        - aes256-gcm@openssh.com
        - aes256-ctr
        - aes256-cbc
        - rijndael-cbc@lysator.liu.se
        - aes192-ctr
        - aes192-cbc

        - aes128-gcm@openssh.com
        - aes128-ctr
        - aes128-cbc
        - 3des-cbc
- SftpClientKexAlgorithms - Override client's enabled KEXes and their order Example: "SftpClientKexAlgorithms" : "ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha256" The combined values should be comma separated *without* any additional characters. (If not set, then it uses default ordering which is same as server inbound order.)
    - For non-FIPS, SftpClientKexAlgorithms, you can combine values:
        - ecdh-sha2-nistp521
        - ecdh-sha2-nistp384
        - ecdh-sha2-nistp256
        - diffie-hellman-group18-sha512
        - diffie-hellman-group16-sha512
        - diffie-hellman-group14-sha256
        - diffie-hellman-group-exchange-sha256
        - diffie-hellman-group14-sha1
        - curve25519-sha256
        - curve25519-sha256@libssh.org
        - sntrup4591761x25519-sha512@tinyssh.org
        - diffie-hellman-group-exchange-sha1
        - diffie-hellman-group1-sha1
    - For FIPS, SftpClientKexAlgorithms, it is possible to combine some of the values:
        - ecdh-sha2-nistp521
        - ecdh-sha2-nistp384
        - ecdh-sha2-nistp256
        - diffie-hellman-group18-sha512
        - diffie-hellman-group16-sha512
        - diffie-hellman-group14-sha256
        - diffie-hellman-group-exchange-sha256
        - diffie-hellman-group14-sha1
        - diffie-hellman-group-exchange-sha1

- SftpClientMACs string - Override client's enabled MACs and their order. Example: "SftpClientMACs": "hmac-sha2-256,hmac-sha2-512,hmac-sha1" The combined values should be comma separated *without* any additional characters. (If not set, then it uses default ordering which is same as server inbound order.)
    - For non-FIPS, SftpClientMACs, you can combine values:
        - hmac-sha2-512-etm@openssh.com
        - hmac-sha2-512
        - hmac-sha2-256-etm@openssh.com
        - hmac-sha2-256
        - hmac-sha1-etm@openssh.com
        - hmac-sha1
        - umac-64-etm@openssh.com
        - umac-64@openssh.com
        - hmac-md5
        - hmac-sha1-96
        - hmac-md5-96
    - For FIPS, SftpClientMACs, you can combine values:
        - hmac-sha2-512-etm@openssh.com
        - hmac-sha2-512
        - hmac-sha2-256-etm@openssh.com
        - hmac-sha2-256
        - hmac-sha1-etm@openssh.com
        - hmac-sha1

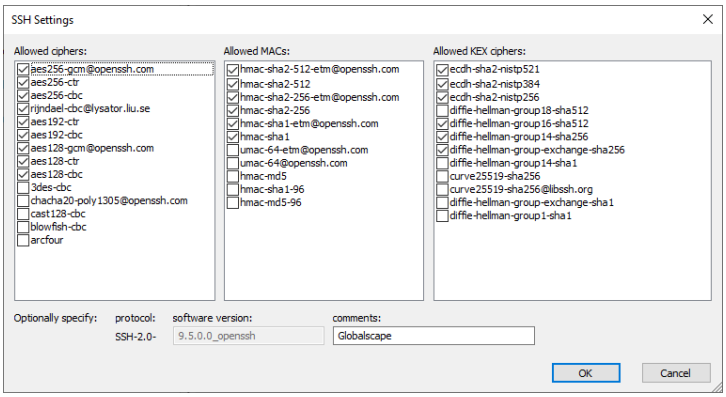
Related Topics

- Viewing or Modifying MAC Settings
- https://kb.globalscape.com/Knowledgebase/11092
- https://kb.globalscape.com/Knowledgebase/11338
- https://kb.globalscape.com/Knowledgebase/11385
- https://kb.globalscape.com/Knowledgebase/11266
- https://kb.globalscape.com/Knowledgebase/11456

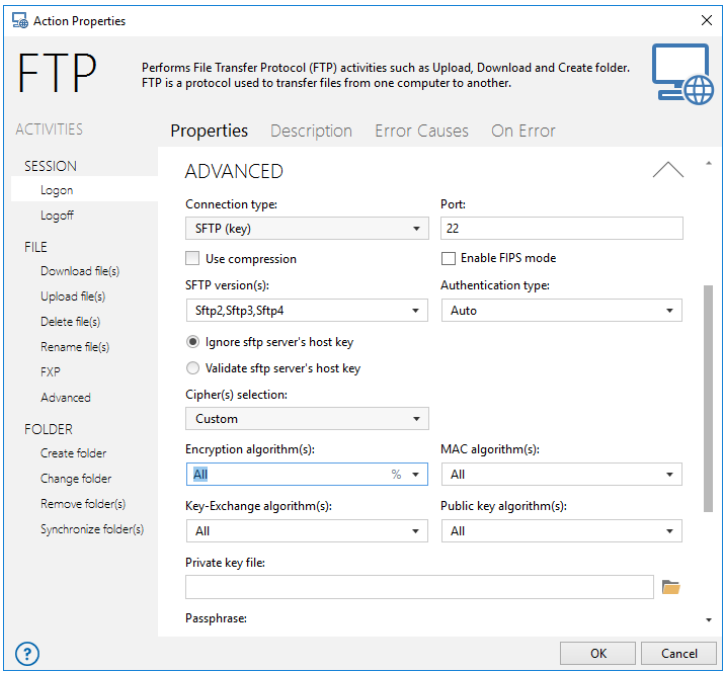
SFTP Encryption Algorithms

Numerous SFTP encryption algorithms are available in EFT and the Advanced Workflows module. It is up to you to determine which settings to use in your environment.

In EFT, click the server node, **Security** tab > **SFTP security settings** > **Configure**:



The encryption algorithms, key-exchange algorithms, and MAC algorithms supported by Automate are listed in their FTP - Log On Action, under **Advanced**. Click the drop-down lists to the **Encryption algorithms**, **MAC algorithms**, **Key-Exchange algorithms**, and **Public key algorithms** available.

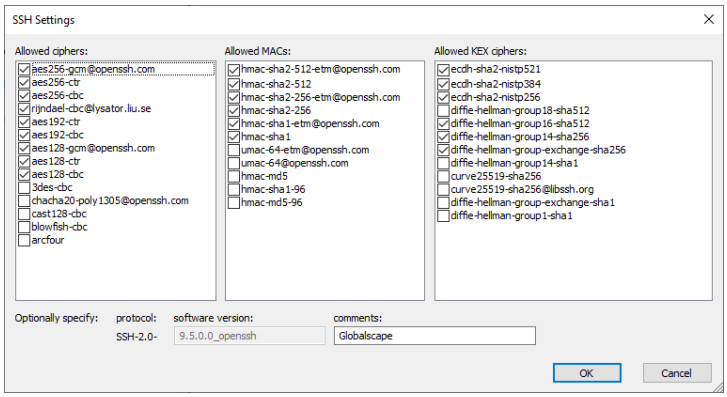


Enabling SFTP (SSH) on the Server

Specify ciphers, macs, and KEX ciphers before enabling SFTP connections. After you have enabled SFTP for the server, SFTP connections can be enabled on the Site, Settings Template, and/or for each user. Each level can inherit the settings from the parent.

To configure SFTP on the Server

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the server node that you want to configure.
3. In the right pane, click the **Security**tab.
4. Next to **SFTP security settings**, click **Configure**. The **SSH Settings** dialog box appears.



5. Select the check box of one or more ciphers, macs, and KEX ciphers to use; clear check boxes of ciphers, macs, and KEX ciphers that you don't want to use. At least one cipher must be specified.
6. Click **Apply**to save the changes to EFT.

The EFT SFTP library implementation is based on the 8.1 version of OpenSSH portable: https://github.com/PowerShell/openssh-portable, which is a fork of https://github.com/openssh/openssh-portable, which in turn is a fork of the canonical OpenSSH. EFT will be updated once the fork that EFT is using is updated to 8.2, 8.3, or newer version. Also note that the EFT implementation contains some modified OpenSSH files, modified via use of a Fedora patch, for purposes of FIPS certification when FIPS mode is enabled (where EFT leverages OpenSSL's LibEay32.dll for SFTP's cryptographic functions).

Creating an SSH Key Pair

(Requires the SFTP module) In the administration interface, you can define an SSH key pair for EFT and connecting clients. A wizard walks you through each step to create and store the key pair files.

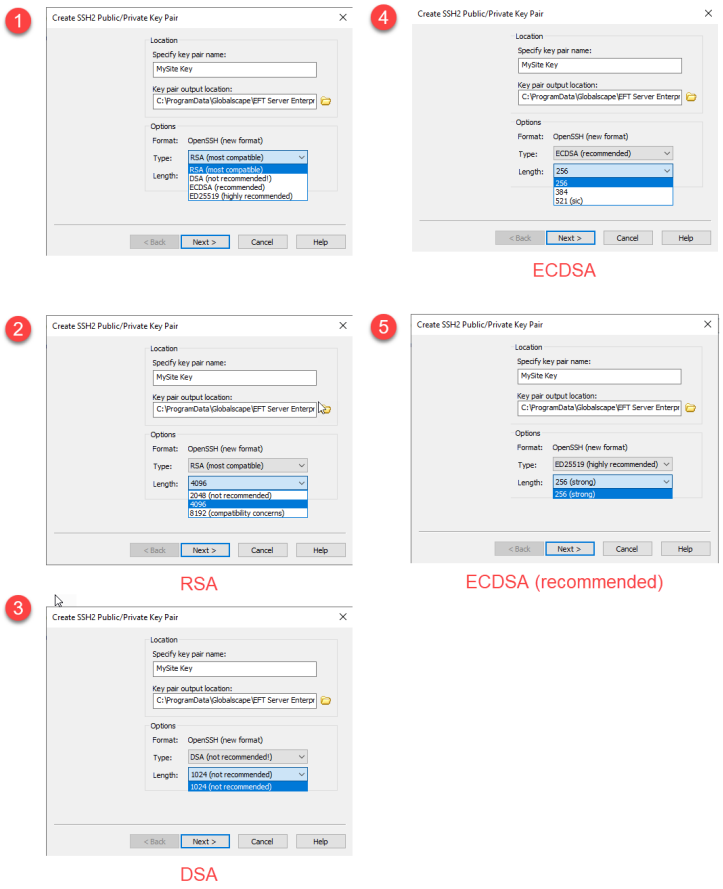
For the KEX ciphers, there a few configuration changes to note:

- On a new installation, diffie-hellman-group-exchange-sha256 and diffie-hellman-group14-sha1 should be enabled.
    - diffie-hellman-group14-sha1 should be left enabled for compatibility in accordance with the most recent SSH RFC draft recommendations (dated March 27th, 2017):
      "diffie-hellman-group14-sha1 method SHOULD- be retained for compatibility with older Secure Shell implementations. It is intended that this key exchange method be phased out as soon as possible"
      https://tools.ietf.org/html/draft-ietf-curdle-ssh-kex-sha2-07
- On upgrade, existing selected KEX methods should persist.
- An advanced property to disable/enable diffie-hellman-group1-sha1 (https://kb.globalscape.com/KnowledgebaseArticle11266.aspx) should become inactive in place of the administration interface selections.

To create a key pair

1. On the main menu, click **Tools >Create SSH2 Key**.

   The **Create SSH2 Public/Private Keypair** wizard appears.



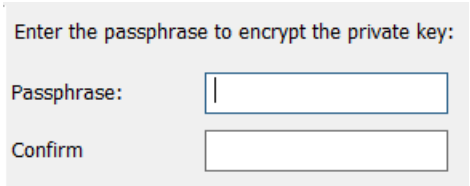
2. Specify a name for the key pair. The default is "New SSH Key," but you can name it anything. (You are prompted to specify a different name if a key with the same name exists.)
3. Specify a location in which to store the key pair.
4. In the **Options**area:
   - Select the length.
   - Select the type (algorithm):

     You can choose the algorithm and bit length when creating new keys.

Algorithm	Length
RSA (most compatible)	2048 (not recommended) 4096 8192 (compatibility concerns)
DSA (not recommended!)	1024 (not recommended)
ECDSA (recommended)	256 384 521 (sic)
Ed25519 (highly recommended)	256 (strong)

RSA 4096 are the defaults for new installations. See https://www.ssh.com/ssh/keygen/ for more information. Key algorithms with a single choice show that length value appears dimmed, as those cannot be edited.

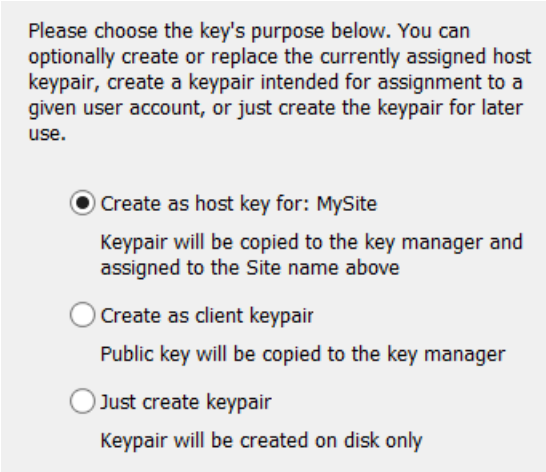
5. Click **Next**. The password page of the wizard appears.



6. Provide and confirm the passphrase used to encrypt the private key. The passphrase cannot contain more than 256 characters, cannot contain only spaces and periods, and ***cannot***contain the following characters:

/ (forward slash)	**:** (colon)	**?** (question mark)
**** (back slash)	**|** (pipe)	**<** (left angle bracket)
[(left bracket)	**=** (equal sign)	**>** (right angle bracket)
] (right bracket)	**,** (comma)	**{** (left curly brace)
; (semicolon)	**+** (PLUS sign)	**}** (right curly brace

7. Click **Next**.



8. Choose the key's purpose:
   - If you want to use this key to authenticate EFT for inbound transactions, click **Create as host key for: <Site Name>**.
     The keypair is copied to the SSH Key Manager and assigned to the Site on which you create the key.
   - If you want EFT to import the public part of the key into the SSH key manager, click **Create as client keypair**.
     The private key for client is stored on client's side. EFT doesn't store it. It is the administrator's responsibility to securely send this private key to a user, so the user can use it with SFTP clients (for example, CuteFTP®).
   - If you only want to create a keypair on disk, click **Just create keypair**.

     Copying the public key to the key manager is unnecessary unless you created this key pair for your partner. For security best practices, your partners should create their own key pairs, then give you a copy of their public key, which you would then import into the SSH key manager.

9. Click **Finish**. If you used the default location to store the key pair, the files are is saved in **C:\ProgramData\Globalscape\EFT Server**.

PowerShell Example

Refer to the COM API helpfor details of using the CreatSSHKeyPair method.

In PowerShell, use the following example:

```
$privateKeyFile = New-Object Object
$publickKeyFile = New-Object Object
 #define VariantWrapper for variables to be passed as VARIANT
 $wrappedPublic = New-Object
 Runtime.InteropServices.VariantWrapper($publickKeyFile)
 $wrappedPrivate = New-Object
 Runtime.InteropServices.VariantWrapper($privateKeyFile)
#pass a [ref]VariantWrapper to .COM method
$site.CreateSSHKeyPair($ssha_rsa_type+$keyBits,
"siteSSHKeyPass", [ref]$wrappedPublic, [ref]$wrappedPrivate)
```

Available MACs

The following are a list of available MACs

- hmac-sha2-512-etm@openssh.com (enabled by default/secure) Added in v8.0.4
- hmac-sha2-512 (enabled by default/secure)
- hmac-sha2-256-etm@openssh.com (enabled by default/secure) Added in v8.0.4
- hmac-sha2-256 (enabled by default/secure)
- hmac-sha1-etm@openssh.com (enabled by default/secure) Added in v8.0.4
- hmac-sha1 (enabled by default/secure)
- umac-64-etm@openssh.com (enabled by default) Added in v8.0.4
- umac-64@openssh.com (enabled by default)
- hmac-md5 (disabled by default/less secure) In v8.0.2, this MAC was changed to disabled
- hmac-sha1-96 (disabled by default/less secure) In v8.0.2, this MAC was changed to disabled
- hmac-md5-96 (disabled by default/less secure) In v8.0.2, this MAC was changed to disabled

The MACs below can be enabled/disabled by changing their Advanced Properties in the AdvancedProperties.json

Advanced Property	Description
SFTP2_HMAC_SHA2_512_ETM_AT_OPENSSH_COM	Type: bool Default Value: true Description: Setting to true enables the hmac-sha2-512-etm@openssh.com algorithm. Can be disabled for outbound client connections via Advanced Property SFTP2_HMAC_SHA2_512_ETM_AT_OPENSSH_COM to false

Advanced Property	Description
SFTP2_SHA2_512	Type: bool Default Value: true Description: Setting to true enables the SHA2_512 MAC algorithm. hmac-sha2-512 can be disabled for outbound client connections via Advanced Property SFTP2_SHA2_512 to false
SFTP2_HMAC_SHA2_256_ETM_AT_OPENSSH_COM	Type: bool Default Value: true Description: Setting to true enables the hmac-sha2-256-etm@openssh.com algorithm hmac-sha2-256-etm@openssh.com can be disabled for outbound client connections via Advanced Property SFTP2_HMAC_SHA2_256_ETM_AT_OPENSSH_COM to false
SFTP2_SHA2_256	Type: bool Default Value: true Description: Setting to true enables the SHA2_256 MAC algorithm. hmac-sha2-256 can be disabled for outbound client connections via Advanced Property SFTP2_SHA2_256 to false
SFTP2_HMAC_SHA1_ETM_AT_OPENSSH_COM	Type: bool Default Value: true Description: Setting to true enables the hmac-sha1-etm@openssh.com algorithm. hmac-sha1-etm@openssh.com can be disabled for outbound client connections via Advanced Property SFTP2_HMAC_SHA1_ETM_AT_OPENSSH_COM to false
SFTP2_SHA1	Type: bool Default Value: true Description: Setting to true enables the SHA1 MAC algorithm. hmac-sha1 can be disabled for outbound client connections via Advanced Property SFTP2_SHA1 to false

Advanced Property	Description
SFTP2_UMAC_64_ETM_AT_OPENSSH_COM	Type: bool Default Value: true Description: Setting to true enables the umac-64-etm@openssh.com algorithm. umac-64-etm@openssh.com can be disabled for outbound client connections via Advanced Property SFTP2_UMAC_64_ETM_AT_OPENSSH_COM to false
SFTP2_UMAC_64_AT_OPENSSH_COM	Type: bool Default Value: true Description: Setting to true enables the umac-64@openssh.com algorithm. umac-64@openssh.com can be disabled for outbound client connections via Advanced Property SFTP2_UMAC_64_AT_OPENSSH_COM to false
SFTP2_MD5	Type: bool Default Value: false Description: Setting to true enables the MD5 MAC algorithm. hmac-md5 can be ENABLED for outbound client connections via Advanced Property SFTP2_MD5 to true
SFTP2_SHA1_96	Type: bool Default Value: false Description: Setting to true enables the SHA1_96 MAC algorithm. hmac-sha1-96 can be ENABLED for outbound client connections via SFTP2_SHA1_96 to true
SFTP2_MD5_96	Type: bool Default Value: false Description: Setting to true enables the MD5_96 MAC algorithm. hmac-md5-96 can be ENABLED for outbound client connections via Advanced Property SFTP2_MD5_96 to true

Related Topics

- EFT SFTP Key Support
- EFT SSH Key Formats
- Configuring SFTP for a Site
- Creating an SSH Key Pair
- Viewing or Modifying Message Authentication Codes (MAC) Settings
- Creating SFTP Algorithms
- Viewing, Importing, Renaming, and Deleting Client Keys
- Modifying the SFTP Identification String

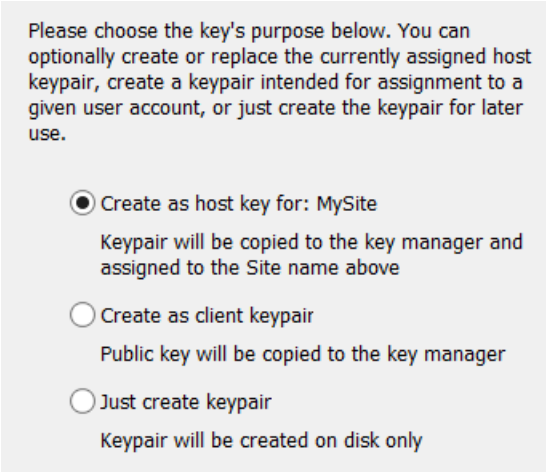
Configuring SFTP for a Site

(Requires the SFTP module) When you enable SFTP for a Site, you must configure the SFTP settings. You can then configure SFTP options for a Settings Template and/or user account.

Before upgrading from a version prior to v8.x, *export and convert your SFTP keys. The new version only creates RSA keys in OpenSSH new format. (You can't generate DSS keys and save keys in SSH.com format.)* See also SFTP FIPS.

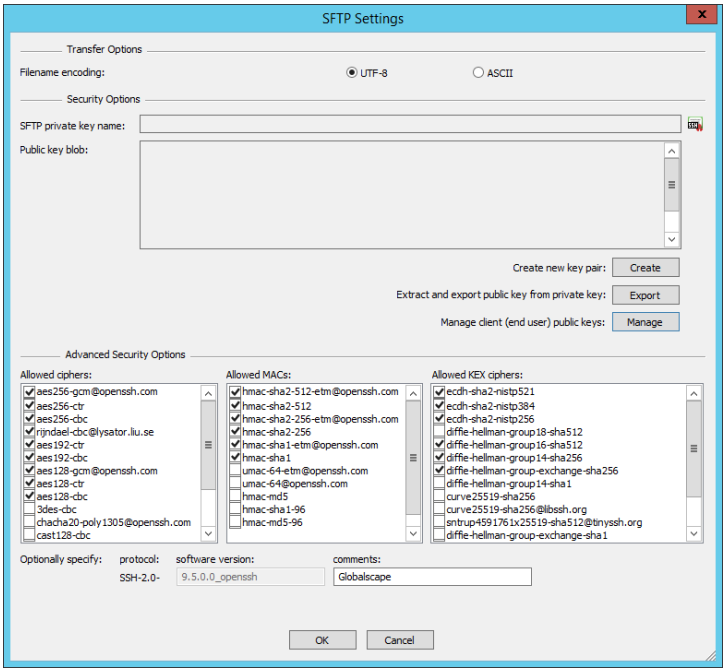
To configure SFTP for a Site

1. Before you can enable and configure SFTP on the Site, you must create or importan SFTP key defined on the Site. Be sure to select **Create as host key for: <site_name>** before you click **Finish**.



2. In the administration interface, connect to EFT and click the **Server**tab.
3. On the **Server**tab, click the **Site** you want to configure, then click the **Connections**tab.

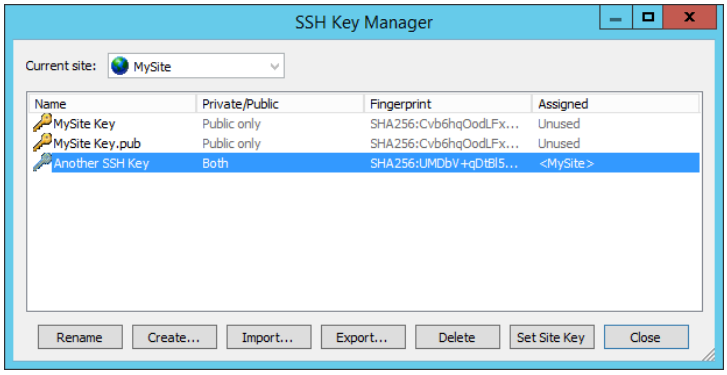
4. Click **SFTP Config**. The **SFTP Settings** dialog box appears.



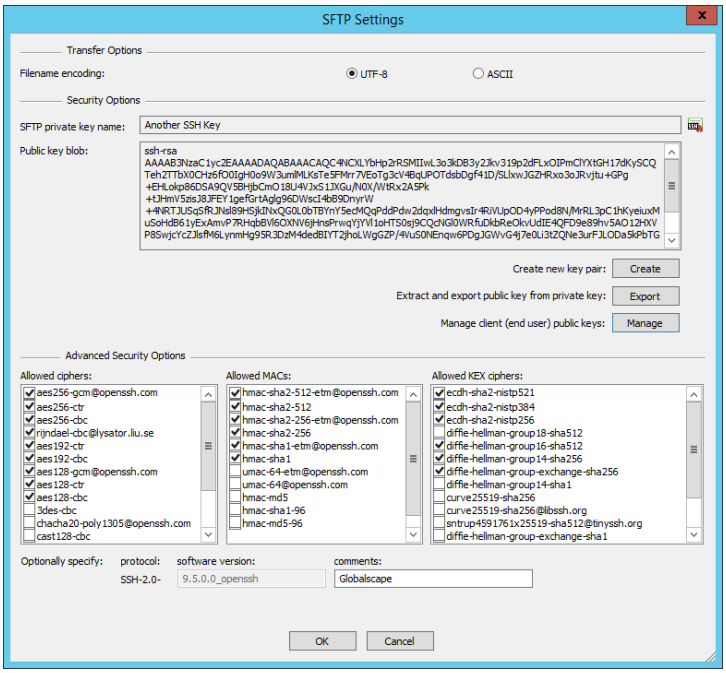
EFT's SFTP library implementation is based on the 8.1 version of OpenSSH portable: https://github.com/PowerShell/openssh-portable, which is a fork of https://github.com/openssh/openssh-portable, which in turn is a fork of the canonical OpenSSH. EFT will be updated once the fork that EFT is using is updated to 8.2, 8.3, or newer version. Also note that the EFT implementation contains some modified OpenSSH files, modified via use of a Fedora patch, for purposes of FIPS certification when FIPS mode is enabled (where EFT leverages OpenSSL's LibEay32.dll for SFTP's cryptographic functions).

- If you enabled SFTP and created keys when you defined the Site, the key name and blob appear in the **SFTP Settings**dialog box.
- If you did not enable SFTP when you created the Site, the dialog box is empty. Refer to Creating an SSH Key Pair for instructions to create the keys, if necessary.

5. If you have multiple SFTP keys, click the SSH icon to the right of the **SFTP private key name** box. The **SSH Key Manager** dialog box appears.



6. In the **SSH Key Manager**dialog box, click the Private/Public key that you want to assign to the Site, click **Set Site Key**, then click **Close**. The assigned SFTP private key name and blob appear in the dialog box.



7. In the **Filename encoding**area, click **UTF-8** or **ASCII**.
   - **UTF-8**—For Unicode-only transfers
   - **ASCII**—Detects whether to proceed in ASCII mode or switch to UTF-8 mode for the transmission and receipt of path names and other strings communicated between client and server.
8. Click **OK** to close the dialog box.
9. Click **Apply**to save the changes.

Related Topics

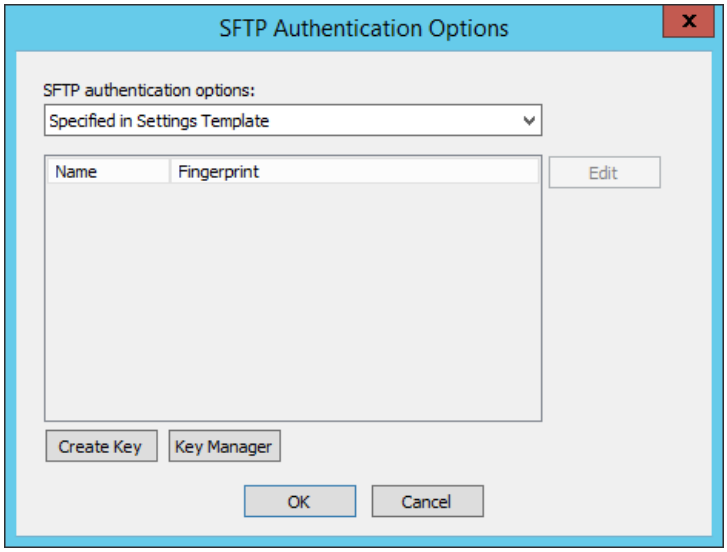
- SFTP Key Support
- SFTP Logging
- SSH Key Formats
- Creating an SSH Key Pair
- Viewing or Modifying Message Authentication Codes (MAC) Settings
- Specifying SFTP Algorithms
- Configuring User SFTP Authentication
- Managing SFTP Keys for the Site
- Modifying the SFTP Identification String

Configuring User SFTP Authentication Options

(Requires the SFTP module) Enable and configure SFTP on the Site first, then specify the SFTP authentication options for the Settings Template and user accounts. You can assign multiple SSH keys to users.

To specify SFTP authentication options for a user account or Settings Template

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Settings Template or user that you want to configure.
3. In the right pane, click the Connectionstab.
4. In the **Protocols** area, select the **SFTP (SSH2)** check box, then click **SFTP Auth**. The **SFTP Authentication Options**dialog box appears.

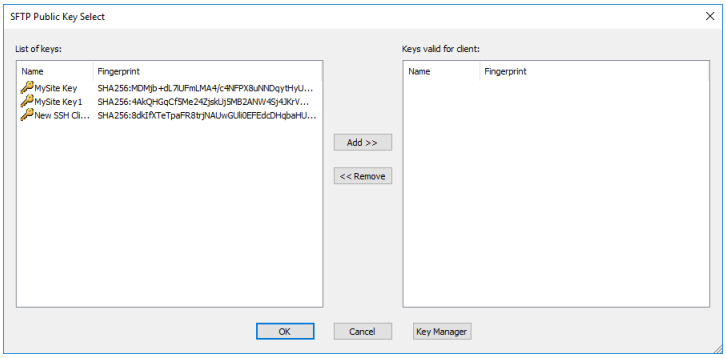


5. In the **SFTP authentication options** list, specify whether user are to connect using **Password only**, **Public key only**, **Public Key & Password**, or **Public key or Password.**

   Compliance with PCI DSS requires that users change their password upon initial login. Because the **Public key only**method does not use a password, it potentially violates the PCI DSS and is, therefore, not available on Sites defined using the "strict security settings" option. You can, however, use the **Public Key and Password** method.

   On Active Directory-authenticated Sites, the **Public Key Only**and **Public key or Password**options are not available, because AD Sites require keyboard authentication.

6. If you selected any option besides **Password only** or **Specified in Settings Template**, click **Edit**. The **SFTP Public Key Select** dialog box appears.



   The SFTP public keys that are defined for this Site appear in the **List of keys**. If no keys appear, click **Key Manager** to import keys.

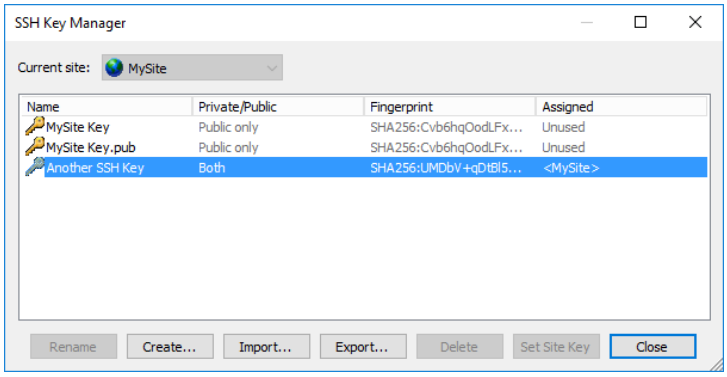
7. In the **List of keys** box, double-click the key(s) to use, or click each key, and then click **Add**. The selected key(s) appear in the **Keys valid for client**list.
   - You can sort the list by Name or Fingerprint. The modifications and changes are lost once the dialog box is closed.
8. Click **OK** to close the **SFTP Public Key Select** dialog box. The selected key(s) appear in the **Authentication key list**.
9. Click **OK** to close the **SFTP Authentication Options**dialog box.
10. Click **Apply**to save the changes on EFT.

Managing SFTP Keys

(Requires the SFTP module)SFTP/SSH Keys defined for a Site appear in the **SSH Key Manager**. The **Key Manager**displays the key name, fingerprint, and Site assigned.

To view, import, rename, or delete keys

1. Open the **SFTP Settings** dialog box.
2. Click **Manage**. The **SSH Key Manager** appears.



- **Name** - Displays the name of the key. When a key is imported, no assigned names are displayed
- **Private/Public** - Displays Both when the SSH key is assigned to the Site; Private if it is for client access
- **Fingerprint** - Displays the fingerprint of the key
- **Assigned** - Displays the Site assigned to the key

  To assign one or more users to a key, refer to Configuring SFTP Authentication Options.

3. Do one of the following:
   - **To sort keys**, click the **Name** or the **Fingerprint** column.
   - **To import keys**, click **Import**, then browse for and select the key. You can import any **.pub** file accessible from the computer on which the administration interface is installed.
   - **To delete a key**, click the key in the list, and then click **Delete**. EFT will prompt you to confirm that you want to delete the key.
   - **To rename a key**, click the key in the list, and then click **Rename**, or press F2. The server will verify that the name is unique and prompt you to change it if it is not.

4. Click **Close**to close the **SSH Key Manager**.
5. Click **OK** to close the **SFTP Settings** dialog box.
6. Click **Apply**to save the changes on EFT.

Related Topics

- SFTP Key Support
- SSH Key Formats
- Configuring SFTP for a Site
- Configuring User SFTP Authentication
- Creating an SSH Key Pair
- Viewing or Modifying Message Authentication Codes (MAC) Settings
- Specifying SFTP Algorithms
- Modifying the SFTP Identification String

Encoding for SFTP Transfers

(Requires the SFTP module) You can specify UTF-8 or Auto-detect encoding for SFTP transfers on the Site. For most connecting clients, **Auto-detect**is preferred and is the default.

To configure SFTP encoding for the Site

1. Open the **SFTP Settings** dialog box.
2. In the **Encoding**area, click **UTF-8** or **Auto-detect**.
    - **UTF-8**—For Unicode-only transfers
    - **ASCII**—Detects whether to proceed in ASCII mode or can switch to UTF-8 mode for the transmission and receipt of path names and other strings communicated between client and server.
3. Click **OK** to close the dialog box.
4. Click **Apply**to save the changes on EFT.

Extracting the Public SFTP Key

(Requires the SFTP module) If you require clients to authenticate with a public key to access the Site, you need to provide them with the public key file (.pub). You can extract the public key from the SFTP key on the Connections tab of the Site.

To configure SFTP for a Site

1. Before you can enable and configure SFTP on the Site, you must create or importan SFTP key defined on the Site.
2. Open the **SFTP Settings** dialog box.
3. The key that you created when you defined the Site (if you enabled SFTP and created keys) appears in the **SFTP Settings** dialog box. If you did not enable SFTP when you created the Site, the dialog box is empty.
4. Click **Export**to extract and export the public key (**.pub**). A **Save As** dialog box appears in which you can specify a name and location for the **.pub**file.
5. Click **OK** to close the dialog box.
6. Click **Apply**.

Modifying the SFTP Identification String (Optional)

This procedure is for advanced users; in most cases, you will not need to use this procedure.

(Requires the SFTP module) When an SFTP (SSH) connection has been established, both EFT and the client must send an identification string. This identification string must be in the format:

```
SSH-protoversion-softwareversion SP comments CR LF
```

EFT hard codes "SSH-2.0-" into the string; you provide only the software version and, optionally, comments. The **software version** box must consist of printable US-ASCII characters, with the exception of whitespace characters and the minus sign (-).

To modify the SFTP identification string (optional)

1. Open the **SFTP Settings** dialog box.
2. In the **Optionally specify** area, specify the **software version** and **comments**.
3. Click **OK** to close the dialog box.
4. Click **Apply**to save the changes on EFT.

For more information about modifying the SFTP identification string, refer to http://www.ietf.org/rfc/rfc4253.txtsection 4.2.

Related Topics

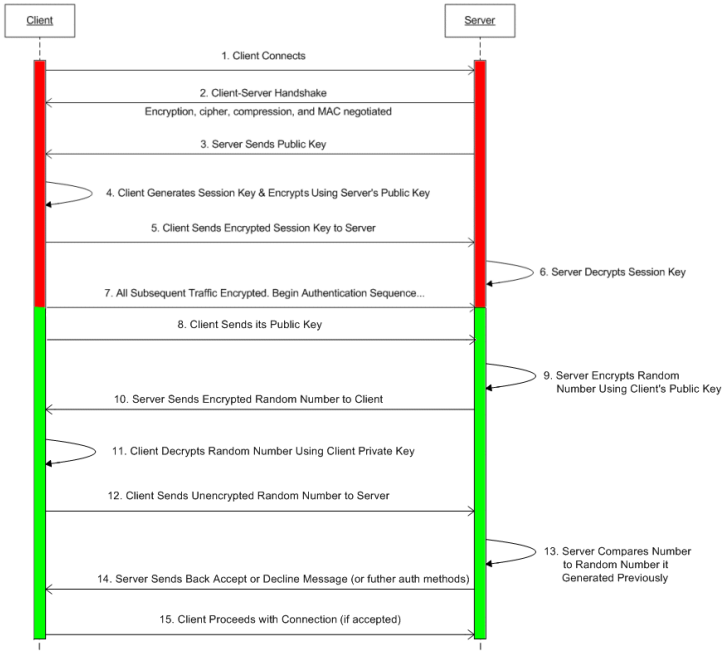
- EFT SFTP Key Support
- EFT SSH Key Formats
- Configuring SFTP for a Site
- Creating an SSH Key Pair
- Viewing or Modifying Message Authentication Codes (MAC) Settings
- Specifying SFTP Algorithms
- Viewing, Importing, Renaming, and Deleting Client Keys
- Modifying the SFTP Identification String

SFTP Key Support

(Requires the SFTP module)EFT supports the following actions for SFTP key support:

- Importing multiple keys stored in a single key file
- Authentication of multiple keys stored in a single key file
- Association of one or more keys to a user account
- Assignment of the same key (or keys) to more than one user account.

Below is an illustration of a basic SFTP transport and SFTP Public Key authentication sequence.



During the client-server handshake, EFT gets the ultimate say in which encryption cipher will be used out of the list of ciphers offered by the client and supported by EFT. For example, assume EFT has the following algorithm list:

```
aes256-cbc,twofish256-cbc,twofish-cbc,aes128-cbc,twofish128-
cbc,cast128-cbc
```

And assume the client sends the following list:

```
blowfish-cbc,aes128-cbc,twofish128-cbc,cast128-cbc,3des-
cbc,arcfour
```

Then the matching cipher will be aes128-cbc, because EFT scans the client list from left to right and looks for the first matching algorithm on EFT, from left to right. To force strong cipher usage, change EFT-supported algorithms to a list that fits your security needs.

Clients often present a single key file that has one or more public keys in it. Some servers read in the first key and ignore any other keys available in the file, which presents a problem if the public key associated with that user's account is found further down in the public key file presented by the connecting user. It also presents a problem when the administrator attempts to import a bunch of keys all located in a single key file.

EFT evaluates where the delimiters are for each key and parses each key until no more keys are found. In the case of client authentication, once a match is made, there is no need to parse the file further (for example, parse first one below, if no match, parse second one, etc., until it reaches the end of file).

EFT maps the selected key (name) to the key assigned to that user, so that when an authentication attempt occurs, it is compared to each mapped key, rather than just a single key. EFT does not hide already selected keys for different users. That is, if you assign **keya.pub**to user jsmith, you can then go and assign that same **keya.pub**to bjones as well.

When EFT imports a key file, each imported key is given the same name as chosen by the administrator upon importing the key. Same name keys are distinguished by their fingerprint and are displayed in the key manager. You can rename keys in the Key Manager.

All user account names mapped to a particular key are displayed in the **Assigned** column in the Key Manager. Multiple user->key assignments are displayed in comma-delimited format in the **Assigned** column in ascending alpha order. By default, when first importing the key, there are no assigned users; assignment occurs in the user account's **Security**tab. You can assign the same key to multiple users, multiple keys to the same user, and multiple keys to multiple users. If any key in the provided key file

matches one of the keys mapped to a user who is attempting to authenticate, the user is authenticated and no further parsing of the key file is done.

Below is a sample **.pub** file containing multiple keys:

```
-----BEGIN RSA PUBLIC KEY-----

mcazCANrC+BCYIywA0I3TVmrv2FTMWo7bpB9rgJx7xGeAZ22JV4IMEI4eCkMor/B

9ADRUDsYDOKA3yZav3Q4yvG8Z3T+hhqJ2hBob+bj8M4e08C3VwmVRz4j4Y+DnvJo

HcKvvmRcd2GvWRN3Q3OQ+QePfaQnUkDxnEWd+mrX1kwGv96GPqmrFREjm0eT966B

qhPtyRa/gNkyoOnXV4/wsXPQb78UnfrFiM0N2CV7v7yj9koaod7p5CCx4ciw4

A5iEWdmInGcGHEgkP/LBuzOfwoXJWGCwttx0AP0FvZL3iplPmGnfKA==

-----END RSA PUBLIC KEY-----

-----BEGIN RSA PUBLIC KEY-----

mRwnVp5OR7FkLOpXEtxE/JBTvhaLDLFGKPHWxS8c4LYIiPHs/Z5arkCsfZbtZNUD

iPbj6QzjjNpAp1HvP0749+CTNTqFLnFAEj9d5YFxXLNWVjz8NwWwNSGH2hvuDOxR

WsixMQg7esHepAvuiwFRyehmhS7wadpdoXxz3dMIFLovxdrhZKSGCOJIUZk5bIjk

OtHn0RQwe8TXYPe3zJvK6s1ank6hPlyhLsqFhn7KueU75ABPV3U2SlboJUPy6DV+

Qk4/B1vcbn4s/Q8Wk1RGZJ5jrGvjT6GcSaQH7y7e4KLzLXlkiSuVFJAqr1nFYa9m

-----END RSA PUBLIC KEY-----
```

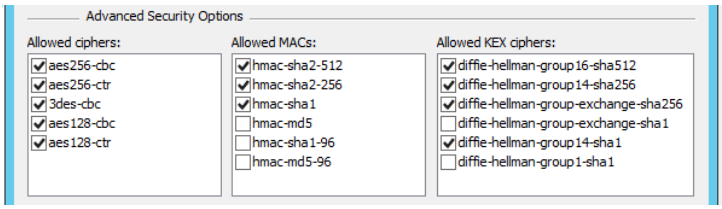
SSH Keys - Security Best Practices

You should not use EFT's key pair in the client, because doing so would involve sending the client the public and private key, potentially creating a security vulnerability. It is also an atypical way of setting up public key authentication for one or more clients. The common practice is to create the key pair in each client and then make the client's public key available to EFT administrator, who in turn should import the client's public key into EFT's trusted list.

SFTP KEX ciphers

EFT supports the following KEX ciphers:

- diffie-hellman-group-exhange-sha256
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1



Related Topics

- Server SSH Key Formats
- Configuring SFTP for a Site
- Creating an SSH Key Pair
- Viewing or Modifying Message Authentication Codes (MAC) Settings
- Specifying SFTP Algorithms
- Viewing, Importing, Renaming, and Deleting Client Keys
- Modifying the SFTP Identification String

Specifying SFTP Algorithms

(Requires the SFTP module) Certain cipher algorithms allow for variable sized keys, while others only allow a specific key size. The length of the key correlates with the strength of that algorithm; larger keys are harder to break than shorter keys. EFT supports the ciphers shown in the **SFTP Settings** dialog box.

To specify encryption algorithms (applies to inbound only)

1. Open the **SFTP Settings** dialog box.
2. In the **Allowed ciphers**list, clear or select the check boxes to specify which ciphers you want to allow for encrypting SFTP sessions.
3. Click **OK** to close the dialog box.
4. Click **Apply**to save the changes on EFT. EFT tries each selected algorithm with the client until one is agreed upon.

Refer to Creating an SSH Key Pair for instructions for creating key pairs, if necessary.

Related Topics

- EFT SFTP Key Support
- EFT SSH Key Formats
- Configuring SFTP for a Site
- Creating an SSH Key Pair
- Viewing or Modifying Message Authentication Codes (MAC) Settings
- Viewing, Importing, Renaming, and Deleting Client Keys
- Modifying the SFTP Identification String

SSH Key Formats

(Requires the SFTP module)EFT imports the PEM format, also called the SECSH Public Key File Format, and the OpenSSH format. Each format is illustrated below. Under the illustrations is a procedure for creating a PEM key on a Linux computer. See also Creating an SSH Key Pair on EFT.

PEM format:

```
---- BEGIN SSH2 PUBLIC KEY ----

Comment: "4096-bit RSA, converted from OpenSSH by don@untu-DSH"

AAAAB3NzaC1yc2EAAAABIwAAAgEAwrr66r8n6B8Y0zMF3dOpXEapIQD9DiYQ6D6/zwor9o

39jSkHNiMMER/GETBbzP83LOcekm02aRjo55ArO7gPPVvCXbrirJu9pkm4AC4BBre5xSLS

7soyzwbigFruM8G63jSXqpHqJ/ooi168sKMC2b0Ncsi+JlTfNYlDXJVLKEeZgZOInQyMmt

isaDTUQWTIv1snAizf4iIYENuAkGYGNCL77u5Y5VOu5eQipvFajTnps9QvUx/zdSFYn9e2

sulWM3Bxc/S4IJ67JWHVRpfJxGi3hinRBH8WQdXuUwdJJTiJHKPyYrrM7Q6Xq4TOMFtcRu

LDC6u3BXM1L0gBvHPNOnD5l2Lp5EjUkQ9CBf2j4A4gfH+iWQZyk08esAG/iwArAVxkl368

+dkbMWOXL8BN4x5zYgdzoeypQZZ2RKH780MCTSo4WQ19DP8pw+9q3bSFC9H3xYAxrKAJNW

jeTUJOTrTe+mWXXU770gYyQTxa2ycnYrlZucn1S3vsvn6eq7NZZ8NRbyv1n15Ocg+nHK4f

uKOrwPhU3NbKQwtjb0Wsxx1gAmQqIOLTpAdsrAauPxC7TPYA5qQVCphvimKuhQM/1gMV22

5JrnjspVlthCzuFYUjXOKC3wxz6FFEtwnXu3uC5bVVkmkNadJmD21gD23yk4BraGXVYpRM

IB+X+OTUUI8=

---- END SSH2 PUBLIC KEY ----
```

EFT looks for the BEGIN and END tags when importing.

OpenSSH format:

If you generated your key on a *nix box, it is most likely in this format.

```
ssh-rsa

AAAAB3NzaC1yc2EAAAABIwAAAgEAwrr66r8n6B8Y0zMF3dOpXEapIQD9DiYQ6D6/zwor9o

39jSkHNiMMER/GETBbzP83LOcekm02aRjo55ArO7gPPVvCXbrirJu9pkm4AC4BBre5xSLS

7soyzwbigFruM8G63jSXqpHqJ/ooi168sKMC2b0Ncsi+JlTfNYlDXJVLKEeZgZOInQyMmt

isaDTUQWTIv1snAizf4iIYENuAkGYGNCL77u5Y5VOu5eQipvFajTnps9QvUx/zdSFYn9e2

sulWM3Bxc/S4IJ67JWHVRpfJxGi3hinRBH8WQdXuUwdJJTiJHKPyYrrM7Q6Xq4TOMFtcRu

LDC6u3BXM1L0gBvHPNOnD5l2Lp5EjUkQ9CBf2j4A4gfH+iWQZyk08esAG/iwArAVxkl368

+dkbMWOXL8BN4x5zYgdzoeypQZZ2RKH780MCTSo4WQ19DP8pw+9q3bSFC9H3xYAxrKAJNW

jeTUJOTrTe+mWXXU770gYyQTxa2ycnYrlZucn1S3vsvn6eq7NZZ8NRbyv1n15Ocg+nHK4f

uKOrwPhU3NbKQwtjb0Wsxx1gAmQqIOLTpAdsrAauPxC7TPYA5qQVCphvimKuhQM/1gMV22

5JrnjspVlthCzuFYUjXOKC3wxz6FFEtwnXu3uC5bVVkmkNadJmD21gD23yk4BraGXVYpRM

IB+X+OTUUI8= don@untu-DSH
```

To make a key

1. To generate the key, on a Linux computer, type:

   ```
   ssh-keygen -t rsa
   ```

2. To convert to PEM format, on a Linux computer, type (assuming your public key is id_rsa.pub):

   ```
   ssh-keygen -e -f id_rsa.pub > yourfilename.pub
   ```

   -i is the inverse of the -e switch

I see the fingerprint in EFT. How do I see the fingerprint in Linux?

Assuming your public key is `id_rsa.pub`, on a Linux computer, type:

```
ssh-keygen -l -f id_rsa.pub
```

This will return three things:

- the bit strength (`4096`)
- the fingerprint (`18:9f:7d:8f:e0:ab:13:56:b7:49:89:b3:07:93:9f:da`)
- the filename (`id_rsa.pub`)

The string returned from this example public key is:

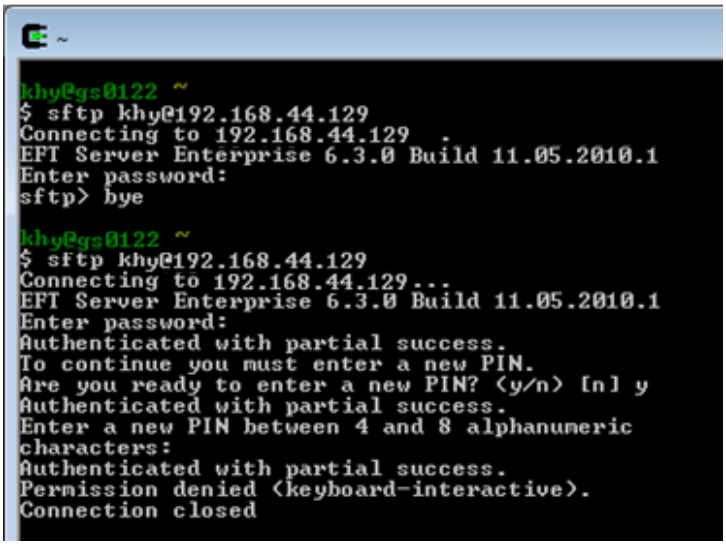
```
4096 18:9f:7d:8f:e0:ab:13:56:b7:49:89:b3:07:93:9f:da id_
rsa.pub
```

Linux has standard folders/files for SSH:

- The SSH files are stored in "~/.ssh"
  The tilde `~`is an alias for the user home folder, e.g., /home/<your username>
- The public key filename is the private key filename with `.pub`as the extension.
- Stored (known) server fingerprints are written to `known_hosts`
  This is used to detect "man in the middle" attacks. If the host fingerprint changes, SSH will report an error.
- The file `authorized_keys`is used to store public keys
  This is used to allow the user to maintain a collection of identity keys in one place (easier to backup and restore). The `authorized_keys`file is a collection of public keys, created by simply echoing out (cat) the contents of a public key, appending it to the bottom of the existing `authorized_keys`file.
- SSH keys must have 600 or more restrictive permissions in place
  If permissions are too open, SSH will report an error and refuse to run until you correct the security problem.

Using SFTP (SSH) with Radius/RSA SecurID

(Requires the SFTP module; two-factor authentication available in AAM)
Authenticating with RADIUS/RSA SecurID can be a multi-step process on your first login, as you establish your PIN. The server can request additional information from the user or device, such as a secondary password. The secondary password prompt can cause problems with SFTP clients who may not allow multiple prompts.



For example, in the screenshot above:

- The first login is a successful login for the user khy (the PIN had already been setup elsewhere).
- The second login attempt by khy is made after the administrator forces PIN setup on the next login (done through the RADIUS/RSA configuration console elsewhere, not in EFT).

To successfully complete the PIN change with OpenSSH SFTP client

- Specify the option:

  ```
  "-oNumberOfPasswordPrompts=N"
  ```

  This option allows multiple password prompts up to the number (N) that you specify.

Refer to the OpenSSH man pages for more information: http://www.manpagez.com/man/5/ssh_config/.

Related Topics

- Adding RADIUS for User Authentication
- Enabling or Disabling RADIUS

Viewing or Modifying Message Authentication Codes (MAC) Settings

(Requires the SFTP module)A keyed-Hash Message Authentication Code (HMAC) is used to verify data integrity and message authenticity, to confirm data has not been altered between the client and the server. SHA (Secure Hash Algorithm) is a cryptographic hash algorithm published by the United States Government. It produces a 160-bit hash value from an arbitrary length string. EFT supports the following HMAC algorithms, which are each selected/enabled by default:

- hmac-sha2-512
- hmac-sha2-256
- hmac-sha1
- hmac-md5
- hmac-sha1-96
- hmac-md5-96

To select Message Authentication Codes (MAC)

1. Open the **SFTP Settings** dialog box.
2. In the **Allowed MACs**list, clear or select the check boxes to specify which algorithms you want to use for message authentication.
3. Click **OK** to close the dialog box.
4. Click **Apply**. EFT tries each selected MAC with the client until an algorithm is agreed upon.

EFT provides advanced properties that affect hmac ciphers:

- hmac-sha2-512 - can be disabled for outbound client connections via Advanced Property SFTP2_SHA2_512 to false
- hmac-sha2-256 - can be disabled for outbound client connections via Advanced Property SFTP2_SHA2_256 to false
- hmac-sha1 - can be ENABLED for outbound client connections via Advanced Property SFTP2_SHA1 to TRUE
- hmac-md5 - can be ENABLED for outbound client connections via Advanced Property SFTP2_MD5 to TRUE
- hmac-sha1-96 - can be ENABLED for outbound client connections via SFTP2_SHA1_96 to TRUE

hmac-md5-96 - can be ENABLED for outbound client connections via Advanced Property SFTP2_MD5_96 to TRUE

If a particular cipher is selected in the interface, both inbound and outbound connections will use that cipher, UNLESS you enable an Advanced Property that changes the behavior for OUTBOUND (EFT acting as client) connections. For the most part, the advanced property is used to turn OFF a specific cipher for outbound that is allowed for inbound; however, in some instances, due perhaps to the security risk involved, the advanced property must enable that algorithm, even if it is already enabled for inbound connections via the interface. This additional step forces administrators to take extra steps for security, and also prevents accidental enabling of a cipher for outbound connections when it was only intended for inbound connections.

Related Topics

- SFTP Advanced Properties
- Server SFTP Key Support
- Server SSH Key Formats
- Configuring SFTP for a Site
- Creating an SSH Key Pair
- Viewing or MAC Settings
- Specifying SFTP Algorithms
- Viewing, Importing, Renaming, and Deleting Client Keys
- Modifying the SFTP Identification String

AS2

(Requires AS2 and HTTP/S module) With the AS2 module, EFT provides the option of transferring files over AS2 (Applicability Statement 2), used to exchange structured business data securely using the HTTP or HTTP/S protocol. The topics below provide an overview of AS2 and describe how to configure EFT's AS2 transfers.

Refer to the *EFT Event Rule Guide* for information about AS2 Events, Conditions, and Actions.

- Introduction to AS2
- How EFT Supports AS2
- AS2 System Requirements
- AS2 Authentication
- Configuring AS2 Transfers
- AS2 Events, Conditions, Actions, and Variables
- AS2 Transaction Auditing and Monitoring
- Testing the AS2 Outbound Connection
- Troubleshooting AS2 Connections
- AS2 Error Warnings and Prompts

Introduction to AS2

(Requires AS2 and HTTP/S modules) AS2 is used to exchange structured business data securely using the HTTP or HTTP/S protocol. Any type of data can be exchanged using AS2, including traditional EDI messages, XML, flat files, spreadsheets, and CAD/CAM data. AS2 is not concerned with the content or validity of the data being sent, but only with the connection and the secure, reliable exchange of data. Data security is achieved using S/MIME through signing and/or encryption.

EDI messages were originally send from an FTP client to an FTP server. The message was not encrypted, and there were no guarantees of receipt or whether it was even sent. With the AS2 protocol, you need a server at both ends of the transmission, the message is encrypted/hashed (over HTTPS), there is verification of who sent/received the message, and data integrity is ensured.

AS2 offers distinct advantages over FTP or plain HTTP, including increased verification and security with receipts and digital signatures. Its transactions and acknowledgments occur in real time, increasing the efficiency of document (data) exchanges. AS2 is also referred to as *EDIINT AS2* (*EDI over the Internet AS2*). Many organizations are migrating to this protocol to reduce costs, and requiring their trading partners to switch to the AS2 protocol. Sending encrypted payloads over HTTPS ensures that only the sender and receiver can view the data exchanged. The use of a hash algorithm ensures data integrity by detecting whether the document was altered during transmission.

The basic structure of an AS2 message can be compared to an envelope that contains a MIME-formatted message inside an HTTP message with AS2 headers. The Message Disposition Notification (MDN) or receipt is returned in the HTTP response message body or in a new message to an alternate URL specified by the originator. This request/reply transactional interchange can provide secure, reliable, and authenticated transport for data using HTTP as a transfer protocol. The security protocols and structures used also support auditable records of these document data transmissions, acknowledgments, and authentication. In a secure message exchange, one organization sends a signed and encrypted message to another organization and requests a signed receipt, and later the receiving organization returns the signed receipt to the sending organization.

Non-repudiation of receipt(NRR) is a legal event that occurs only when the original sender has verified the signed receipt returned from the recipient of the message, and has verified that the returned *message integrity check* (MIC) inside the MDN matches the previously recorded value for the original message. That is, the sender of the message obtains undeniable proof that the recipient received the message and that the message was not altered in transit. NRR is established when both the original message and the receipt use digital signatures.

EFT uses HTTPS to exchange data with AS2-ready servers and clients. Extended HTTP header information outlines how data should be handled and whether signed or unsigned receipts are required.

EFT also validates data integrity upon receipt and requests acknowledgment or *message disposition notification*(MDN) upon completion of outbound transfers. For technical details of AS2, refer to RFC 4130.

Related Topic

- How EFT Supports AS2
- System Requirements
- AS2 Authentication

How EFT Supports AS2

(Requires AS2 and HTTP/S module) EFT incorporates a Drummond-certified integrator to support inbound and outbound AS2 transfers.

EFT uses /n software's EDI Integrator library components, which are in the core of an application called RSSBus. An application is required for certification with Drummond; the components themselves cannot be certified. RSSBus is Drummond Certified and in compliance with RFC4130. That is, the AS2 module itself is not certified; the components used by the AS2 module are certified.

AS2 Optional Profile Supported

EFT supports inbound AS2 Multiple Attachments (MA) for processing a single message with multiple payloads. MA messages are treated the same as normal messages with the exception that multiple files are processed.

EFT also supports the Reliability Profile, which consist of various internal methods for avoiding duplicate file processing standardizes mechanisms for retrying and resending AS2 Messages and MDNs.

What EFT's AS2 module does not support

EFT does not support non-encrypted payloads over plaintext HTTP, asynchronous MDN deliveries via SMTP for outbound transactions (but does support inbound ones), EDI file content manipulation (translation, extraction, transformation, loading), or outbound Multiple Attachments (MA). EFT does not determine if the data sent or received is usable; it only transfers the data. The AS2 module is "push only"; that is, EFT does not request files.

For security reasons, if you are transferring files using HTTP, the payload must be encrypted; if the payload is not encrypted, HTTPS must be used. This Rule applies to both inbound and outbound transactions. Encrypting the payload and sending it over HTTPS provides additional protection from "man-in-the-middle" attacks.

How EFT manages AS2 transmissions

In receiver mode (inbound):

EFT examines the HTTP header, then determines whether to process it as a normal file transfer, as an AS2 receipt (MDN), or as an AS2 transmission. If the file is an AS2 transmission, EFT will process the file, and if a receipt was requested, send a receipt back to the originator. Once the file is received, the following Event triggers will apply:

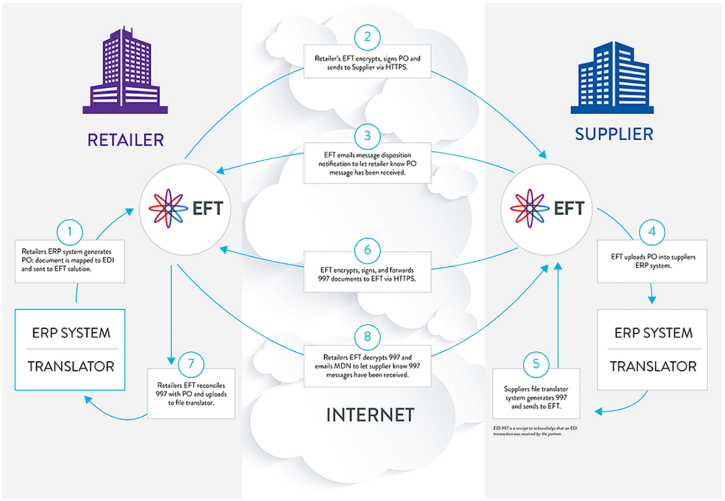
- An On File Upload Event occurs for each file uploaded in an MA transaction.
- An AS2 Inbound Transaction Succeeded Event occurs just once per single file or MA transaction ***after*** all files are received and the MDN (if requested) is successfully sent.
- An AS2 Inbound Transaction Failed Event occurs if an AS2 file upload failed for any reason, such as bad Message Integrity Check (MIC), no permissions/access, duplicate message ID, or other AS2 transfer-related error.

In sender mode (outbound):

EFT provides granular control over AS2 configuration, such as whether to compress or encrypt the message contents, whether to request a synchronous or asynchronous receipt, and whether to launch one or more post transaction Events:

- An AS2 Outbound Transaction Succeeded Event occurs after EFT has successfully offloaded a file to a remote partner and, if a receipt was requested, a valid receipt was received that indicates the transfer was successfully completed.
- An AS2 Outbound Transaction Failed Event occurs if EFT has failed to offload a file to a remote partner, an MDN receipt sent by EFT was not received in the specified duration, or the receipt signature or MIC failed.

EFT sends emails and executes commands only after the final transaction status (Failure or Success) is known. The success or failure to receive the MDN is stored in the database and can be viewed in reports and in the AS2 Status Viewer.



How EFT determines failed AS2 transmissions

AS2 transfers may have more than a simple success or failure outcome. For example, an outbound AS2 file transfer may succeed, but no MDN received from the remote host. This could be considered an outright failure in some cases. Another example of a failure is when a file is successfully sent, but the received MDN's signature cannot be verified. Not all AS2 systems consider these partial failures an overall failure. For example, a remote host may accept an inbound file even though its signature was bad or had other issues, yet still accept the file.

EFT accepts most AS2 transmissions, even if there is a MIC mismatch or the signature used to sign the payload was not found. However, the overall transaction is not considered a success unless every part of the transmission succeeds. That is, EFT's acceptance of the transmission does not mean that the transmission was successful.

EFT's implementation of AS2 considers the following transmissions permanent failures:

- An inbound unencrypted transmission over plaintext HTTP protocol
- An upload attempt to a folder to which the user does not have write permission

In each of these situations, the transmission is rejected automatically. An error is returned to the client, audited to the database, and can trigger an AS2 transaction failure Event, if configured.

Redirecting AS2 transfers from HTTP to HTTPS

You can configure EFT to redirect HTTP connections to HTTPS. The redirect HTTP to HTTPS option affects all incoming HTTP transmission including AS2 requests over HTTP. When you have configured redirection, EFT simply tells the connecting client

that the resource was moved to the new HTTPS URL. The connecting client decides whether it will allow the redirect, because the new URL could be on different server. If the connecting AS2 client does not allow redirection to a different port, the connection will fail.

You can also configure EFT to accept AS2 transactions over HTTP/S, but not allow general HTTP and/or HTTPS transactions. To do this, simply turn off HTTP and/or HTTPS and turn on AS2. The HTTP engine will stay active and only process HTTPS requests that include the AS2 headers.

Are AS2 transfers FIPS certified?

If FIPS is enabled for SSL in EFT, then AS2 transfers over HTTPS use FIPS-certified encryption for the SSL/TLS connection through the Internet. Internal processing of the AS2 MIME payload, may use non-FIPS algorithms or hashes, such as MD5, depending on the content of the AS2 payload or MDN that is received. The module itself is not FIPS certified.

EFT supports the signature and MDN algorithms in the EDI component:

- sha1
- md5
- sha-256
- sha-384
- sha-512
- sha-224

AS2 and ARM

The Auditing and Reporting module (ARM) is not required, but is recommended for auditing purposes. (The receipt policy is not dependent on ARM.) AS2 transfer data is stored in the database, but does not affecte the receipts of the transaction. EFT also provides details on the transactions on the **Status** tab. Refer to Transfers - AS2 Status Viewer for details.

AS2 Authentication

(Requires AS2 and HTTP/S module)) In "normal" authentication, EFT supports client-authenticated transactions, meaning EFT's HTTP/S protocol handler requires a username and password at the outset of the HTTP/S-based AS2 transaction. After it authenticates the partner's login credentials, EFT passes the transaction to its AS2 processor, which performs all message validation and handling. This normal authentication method is secure, but requires the administrator to create and manage partner accounts.

If you are using ***To specify SSL certificate-based logins for the Settings Template or a User* on page 438** for accounts that need to send AS2 transfers, leave it at the default password authentication, not certificate authentication.

Message Level Security (MLS) authentication is a sort of sub-set of normal authentication. MLS requires only two criteria to authenticate on EFT (AS2-From + signature), whereas normal authentication can require up to four criteria (Username + Password + AS2-From + Signature).

To accommodate MLS, instead of immediately rejecting messages that don't contain the Authentication verb (or an empty value next to the Authentication verb) EFT manually looks for the **AS2-From** verb, and if present, looks up the partner account that matches the identifier. If that account is found, and if MLS is allowed for that partner, EFT passes the message to its AS2 processor, along with the mandatory "RequireSign" parameter--one of two mandatory factors used for MLS authentication. The AS2 processor checks for mismatched signatures and properly formatted AS2 messages, and if validated, submits the transaction to the AS2 engine for decryption and processing.

Regardless of whether MLS is enabled for a particular partner account, if a username and password are provided (authentication verb and values present), EFT validates the user account credentials. If those credentials are invalid, the transaction is denied (regardless of whether the **AS2-From** and signatures match). If the credentials are valid, then the transaction proceeds and is passed to the AS2 processor. However, if MLS authentication is enabled for that partner, then not only does the **AS2-From** identifier have to match up with that partner account, but also the RequireSign must be passed to the AS2 processor (and be a valid signature for that account), meaning all four factors must be correct. If, on the other hand, normal authentication mode was specified for the user (rather than MLS), then only the username and password factors are checked, unless **AS2-From** and signature factors were required by EFT, as specified in the inbound settings for that particular partner's account.

Process flow:

If authentication credentials are missing, EFT manually parses the **AS2-From** ID, and then:

- If not present rejects the transaction
- If present, locates the partner (user) account associated with the **AS2-From** ID
  - If no partner is found, EFT rejects the transaction
  - If a partner is found, EFT determines if MLS is allowed for that partner
    - If MLS is not allowed, EFT rejects the transaction
    - If MLS is allowed, EFT passes the transaction to the AS2 component for processing, along with the RequireSign parameter set to True

If authentication credentials are present, EFT validates the credentials, and then:

- If invalid, EFT rejects the transaction
- If valid, EFT determines if that account will accept or reject mismatched **AS2-From** IDs
  - If set to reject, then EFT verifies the **AS2-From** ID provided in the header matches the account profile **AS2 From** ID
    - EFT rejects the transaction if they do not match
    - EFT accepts the transaction if they do match
- If the **AS2-From** ID is valid, EFT determines whether that account accepts or rejects messages that lack signatures
  - If set to reject, EFT sets RequireSign to true
  - If set to accept, EFT sets RequireSign to false, then submits the transaction to the AS2 component for processing

To mitigate the risk of DoS attacks and prevent unauthorized transactions, the administrator should employ EFT's ***Controlling Access to the Site by IP Address*** **on page 847**, ***Setting Maximum Transfer Size*** **on page 917** to a reasonable level, or select the ***Enabling SSL on the Site*** **on page 424** check box in the **SSL Certificate Settings** dialog box on the Site's **Connections** tab.

You can enable Message Level Authentication in the AS2 Partner Inbound Wizard or the AS2 Inbound Settings dialog box.

Permutations of Valid Authentication Factors

Normal Authentication

Any of the four combinations below will allow the inbound AS2 transaction:

- USERNAME + PASSWORD (“Auth” + “Message not signed” = ACCEPT + “as2-from mismatch” = ACCEPT)
- USERNAME + PASSWORD + AS2 FROM ID + SIGNATURE (“Auth” + “Message not signed” = REJECT + “as2-from mismatch” = REJECT)
- USERNAME + PASSWORD + AS2 FROM ID (“Auth” + “Message not signed” = ACCEPT + “as2-from mismatch” = REJECT)
- USERNAME + PASSWORD + SIGNATURE (“Auth” + “Message not signed” = REJECT + “as2-from mismatch” = ACCEPT)

MLS Authentication

Any of the two combinations below will allow the inbound AS2 transaction:

- AS2 FROM ID + SIGNATURE (“MLS” + “Message not signed” = REJECT + “as2-from mismatch” = REJECT)
- USERNAME + PASSWORD + AS2 FROM ID + SIGNATURE (“MLS” + “Message not signed” = REJECT + “as2-from mismatch” = REJECT)

The following table describes possible login scenarios, depending on settings specified in the partner’s AS2 inbound configuration page (top row column headings), and depending on the verbs and factors provided by the incoming partner in the HTTP headers (left column row headings).

HTTP Header Information sent from inbound AS2 client to EFT "Auth" = username/password|"Sign" = certificate signature	MLS Auth Allowed	Accept mismatch AS2-From id + Do require sign	Reject mismatch AS2-From id + Do require sign	Accept mismatch AS2-From id + Do require sign	Reject mismatch AS2-From id + Do require sign
No Auth, No Sign, AS2ID invalid	fail	fail	fail	fail	fail
No Auth, No Sign, AS2ID valid	fail	fail	fail	fail	fail
No Auth, Sign invalid, As2ID invalid	fail	fail	fail	fail	fail
No Auth, Sign invalid, As2ID valid	fail	fail	fail	fail	fail
No Auth, Sign valid, As2ID invalid	fail	fail	fail	fail	fail
No Auth, Sign valid, As2ID valid	pass	fail	fail	fail	fail
Valid Auth, No Sign, AS2ID invalid	fail	pass	fail	fail	fail
Valid Auth, No Sign, AS2ID valid	fail	pass	pass	fail	fail
Valid Auth, Sign invalid, As2ID invalid	fail	fail	fail	fail	fail

HTTP Header Information sent from inbound AS2 client to EFT "Auth" = username/password|"Sign" = certificate signature	MLS Auth Allowed	Accept mismatch AS2-From id + Do require sign	Reject mismatch AS2-From id + Do require sign	Accept mismatch AS2-From id + Do require sign	Reject mismatch AS2-From id + Do require sign
Valid Auth, Sign invalid, As2ID valid	fail	fail	fail	fail	fail
Valid Auth, Sign valid, As2ID invalid	fail	pass	fail	pass	fail
Valid Auth, Sign valid, As2ID valid	pass	pass	pass	pass	pass
Invalid Auth, No Sign, AS2ID invalid	fail	fail	fail	fail	fail
Invalid Auth, No Sign, AS2ID valid	fail	fail	fail	fail	fail
Invalid Auth, Sign invalid, As2ID invalid	fail	fail	fail	fail	fail
Invalid Auth, Sign invalid, As2ID valid	fail	fail	fail	fail	fail
Invalid Auth, Sign valid, As2ID invalid	fail	fail	fail	fail	fail
Invalid Auth, Sign valid, As2ID valid	fail	fail	fail	fail	fail

From the table above, you can see that:

- If no username/password is provided (No Auth), and the certificate is either not provided (No Sign) or invalid (Sign invalid), the transaction will fail.
- If the username/password is invalid, no matter what the settings are, the transaction will fail. For example, if you have configured Message Level Security, EFT does not require a username/password. But if an incorrect username/password is provided in the header information, the transaction will fail (to prevent unauthorized transactions).
- The advantage to using MLS authentication is that partners can connect without providing a username/password pair, as long as the certification and AS2 ID are valid.

Configuring AS2 Transfers

(Requires AS2 and HTTP/S module) Configuring AS2 transfers involves enabling AS2 on the Site as an allowed protocol, specifying EFT's AS2 identifier and certificate path, and defining AS2 trading partners (user accounts).

The topics below provide details of configuring AS2 transfers.

- Enabling the AS2 Inbound Listener Service
- AS2 Certificates
- Configuring AS2 Partners
- Configuring AS2 Outbound Partners Using the Wizard
- Configuring AS2 Inbound Partners Using the Wizard
- AS2 Inbound Parameters
- AS2 Outbound Parameters
- Configuring an AS2 Outbound Proxy
- Initiating AS2 Outbound Transactions
- Moving Files Received from AS2 Partners
- Renaming Files Received from AS2 Partners
- AS2 Account Information Web Page
- Specifying a Temporary Folder for AS2 Transfers
- Allowing AS2 Connections to a Site
- Allowing AS2 Connections in the Settings Template or User Account
- AS2 Events, Conditions, Actions, and Variables

Enabling the AS2 Inbound Listener Service

(Requires AS2 and HTTP/S module) You can configure EFT as an *AS2 Receiver*by allowing incoming transactions over the AS2 protocol and providing your AS2 Identifier and encryption and signing certificates to your trading partners. Your trading partners need this information to be able to share files over AS2.

When you configure a new Site, the **Site Setup** wizard provides options for configuring the protocol. After a Site is created, you can enable AS2 by selecting the **AS2**check box on the Site's **Connections**tab. You can enable or disable AS2 for partner (user) accounts on the Settings Template or for a partner account, or by selecting AS2 in the **New User Creation** wizard on the protocol selection page when you create the partner account.

To enable the AS2 inbound listener service, you will need to provide the following information:

- **AS2 identifier**. There is no standard for the AS2 Identifier. You can use your name, your company's name, or some other unique name. EFT validates the AS2 identifier to determine whether it is unique (not used by another partner on this EFT). If you type an ID that is not unique, the field resets to blank.

  EFT's AS2 Identifier can be overridden per account (partner); however, if you change EFT's AS2 Identifier, partners will not be able to connect to you until they update EFT's AS2 identifier on their systems.

- **SSL certificate pair path** for signing and encrypting AS2 messages. If the SSL certificate pair does not already exist, you are given the option to create one from within the **AS2 Server Configuration**dialog box.

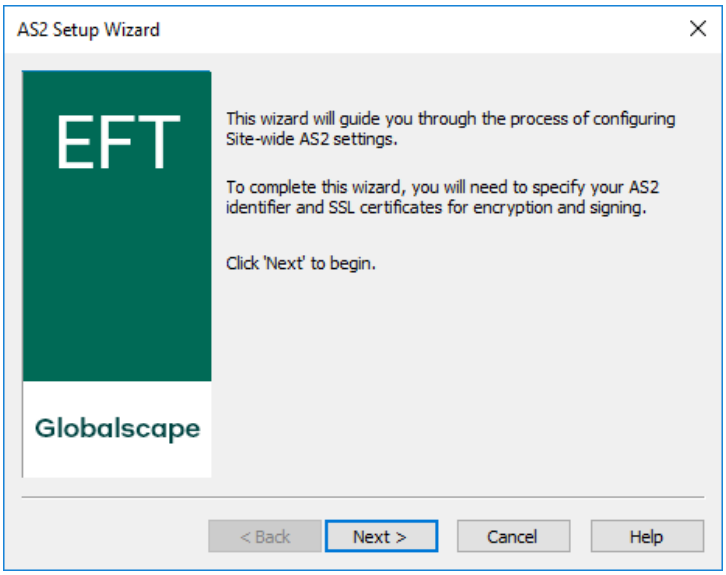
  If you attempt to apply changes, navigate away from the **Connections**tab, or click **OK** in the **Configuration** dialog box when AS2 is enabled and no certificate path has been defined, EFT displays an error message. (You can click **Cancel**to close the dialog box without making changes.)

- EFT and the ARM module must be activated (or trial mode), and the ARM database must be configured.

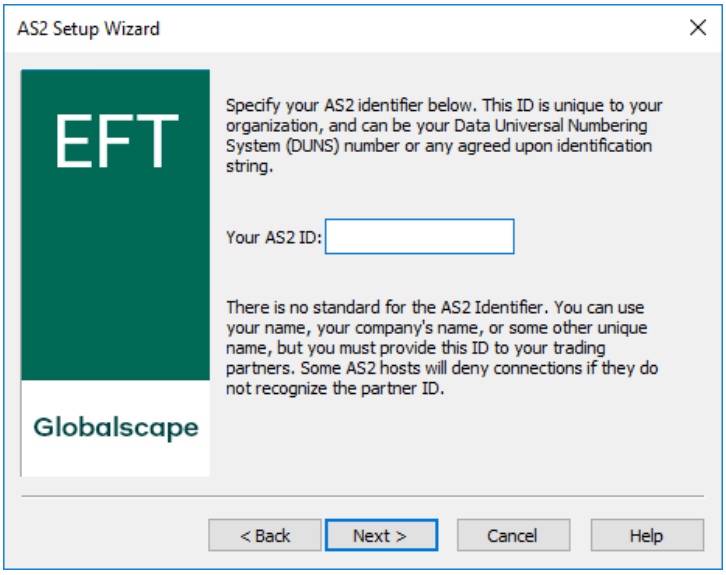
To enable the AS2 inbound listener service

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site that you want to configure.
3. In the right pane, click the **Connections**tab.

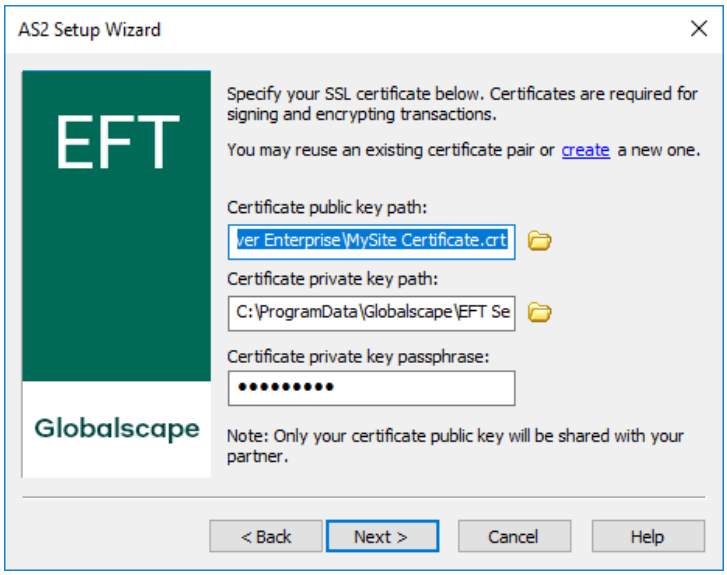
4. Select the **AS2**check box, and then click **AS2 Config**. The **AS2 Setup Wizard** appears.



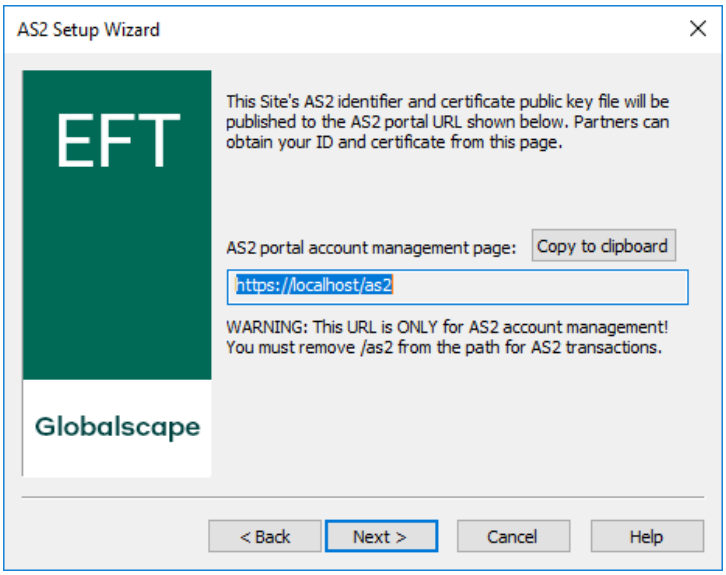
5. Read the **Welcome**page, and then click **Next**. The **AS2 identifier** page appears.



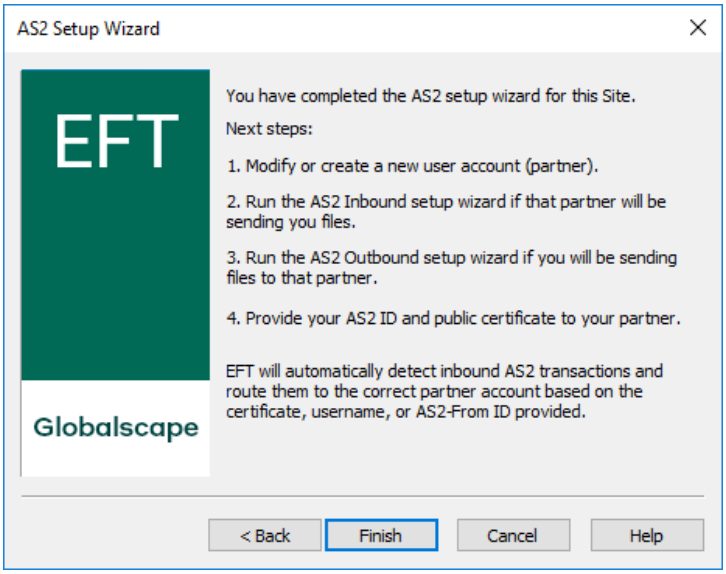
6. In the **Your AS2 Identifier**box, type the name by which you are to be identified to trading partners. (The AS2 ID cannot contain Unicode characters.)
7. Click **Next**. The **Certificate** page appears.



8. Do one of the following:
   - If you do not yet have a certificate defined, click **create**. The **Create certificate**wizard appears.
     a. Follow the prompts in the wizard to create the certificate.
     b. Click **Finish**. The **Certificate file path**, **Private key file path**, and masked **Private key Passphrase**boxes are completed with the location and file names of the created certificate.
   - If you already have a certificate or want to specify a different certificate than the one displayed, specify its location and passphrase as described below:
     a. In the **Certificate file path** box, type the path or click the folder icon to select the file.
     b. In the **Private key file path** box, type the path or click the folder icon to select the file. (Can also be a combined key, e.g. PKCS#12 (.pfx)).
     c. In the **Private key passphrase** box, type the private key passphrase.
9. Click **Next**. The **AS2 portal Web URL** page appears.



10. The **AS2 portal Web URL** can be provided to trading partners so that they can obtain EFT's AS2 identifier and certificate public key to configure their AS2 client to transact with EFT. (You can also deliver the ID and certificate to your partner in an email.)
11. To save the URL to paste into your website or email, click **Copy to clipboard**, then click **Next**. The final page of the wizard appears.



12. Review the **Next steps**, then click **Finish** to save the configuration and close the dialog box.
13. Click **Apply**to save the changes on EFT.

Refer to the topics below for more information regarding configuring AS2 partners and transfers.

Related Topics

- Allowing AS2 Connections to a Site
- AS2 Certificates
- Configuring AS2 Partners
- AS2 Configuration Wizard
- Configuring Inbound AS2 Parameters
- Configuring Outbound AS2 Parameters

AS2 Certificates

(Requires AS2 and HTTP/S module) You can create certificate files using the Certificate wizard. If you have a combined certificate from a third party, use the procedure in Exporting a Certificate from PFX to PEM to extract the public key.

See also: SSL Certificate Compatibility.

Configuring AS2 Partners

(Requires AS2 and HTTP/S module) EFT's AS2 module allows you to setup AS2 partner profiles as user accounts. The profile includes all necessary information for AS2 connectivity, including a *hot folder* that can trigger an event when a file is added using the AS2 profile and send the data that was added. This *partner-provisioning* orientation associates AS2 transactions directly to a user profile, rather than to an event trigger for which you would have to specify the user as a Condition of an Event Rule.

For these user (partner) accounts, the **AS2 Outbound** and **AS2 Inbound** tabs provide the ability to specify an AS2 inbound and outbound policy (parameters) for the selected partner (user). Your trading partners must provide you with the public key of their certificate and their AS2 Identifier.

You can create the accounts manually on the user account tabs or use the AS2 Partner Access wizard to define trading partners with detailed instructions. If you want to configure an AS2 trading partner manually, you first create or determine the Settings Template under which to define the account, create the user account (refer to Configuring Users and Settings Templates), then configure the AS2-specific parameters of the account. (Refer to the **Related Topics** below for the procedures.)

Editing AS2 Partner Profiles

- If you use AD, LDAP, or ODBC authentication and using accounts as AS2 partners, if the account in the external database is changed, deleted, or disabled, any Event Rule or Command that references the account will fail. For example, if the AD account SSmith is renamed SJones, you will have to update any Event Rule or Command manually to reflect the new name of the account.
- If you are using Globalscape authentication and change an account, the Event Rules and Commands that reference the account will also update. However, if you delete or disable the account, or disallow use of AS2 for the account, any Event Rule or Command that references the account will fail. In this case, you should disable or delete the Event Rule, or change the AS2 partner information to an existing/enabled account.

Related Topics

- Configuring AS2 Outbound Partners Using the Wizard
- Configuring AS2 Inbound Partners Using the Wizard
- AS2 Certificates
- AS2 Inbound Parameters
- AS2 Outbound Parameters

- Sending Files via AS2 Partner without Inbound Access
- AS2 Partner Access Wizard

Configuring AS2 Outbound Partners Using the Wizard

(Requires AS2 and HTTP/S module) EFT provides an **AS2 Partner Outbound Wizard** to assist you in configuring AS2 outbound connections. This wizard is accessible from the **AS2 Outbound Settings** dialog box the user account's **Connections**tab, and in the **AS2 Send File**dialog box in the Event Rule Action. The procedure below describes how to use the wizard to configure outbound AS2 partners.

To complete the AS2 Partner Outbound settings, the following information is required:

- Partner's host address used for AS2 transactions
- Partner's AS2 identifier
- Partner's SSL certificate (public key file)
- Login username and password, if required by partner
- Path (inbox, outbox, or mailbox) to the remote server, if required by partner
- Remote proxy settings, if required by partner

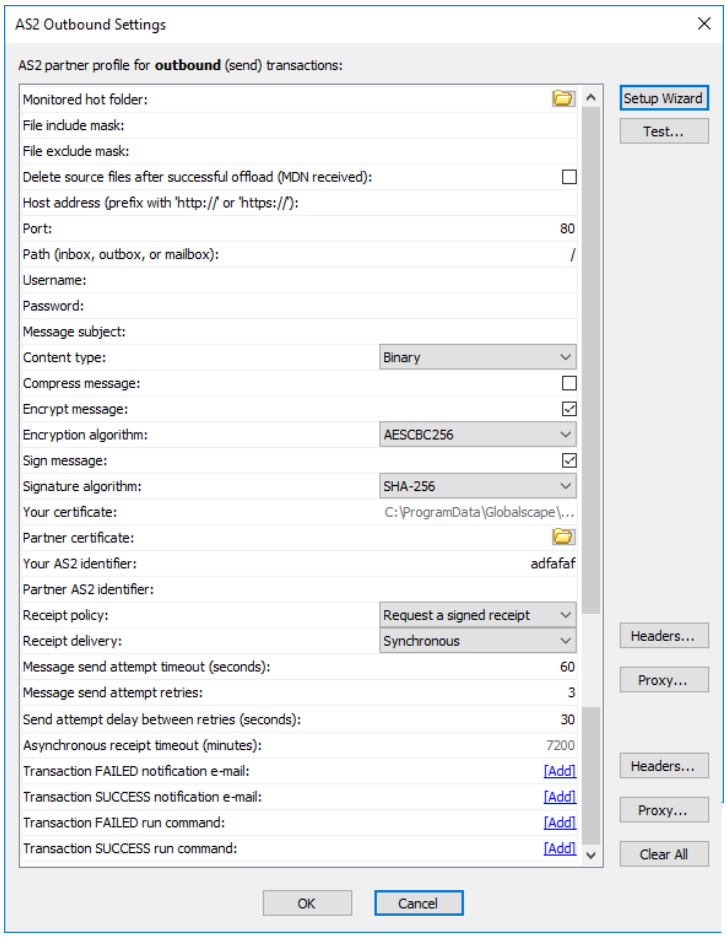
If you plan to execute a command upon success or failure of AS2 transactions, define the command before configuring your partner access; or you can go back later and edit the AS2 partner manually after you have defined the command.

If you plan to send a notification email upon success or failure of AS2 transactions, you can Create an email Notification Template to use in the email Action.

The MDN timeout for an AS2 reply is hardcoded to two hours; 5-day timeout for **asynchronous**transactions. See also the Retry and Timeout options below.

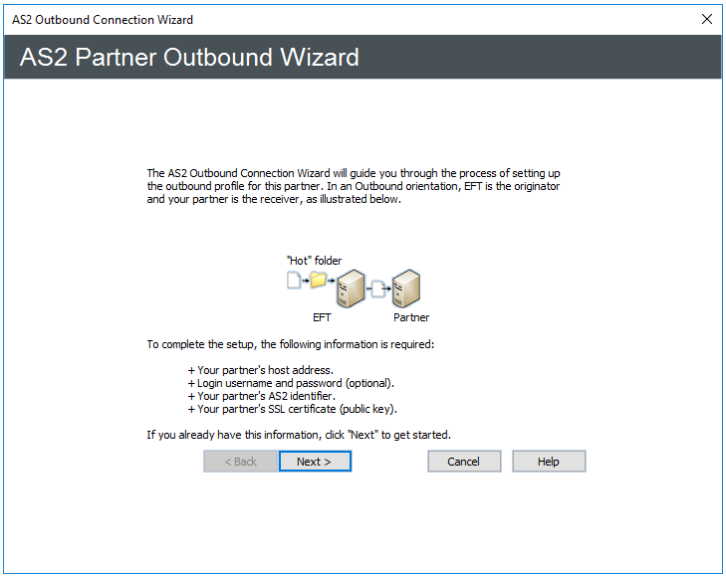
To configure outbound AS2 partners using the wizard

1. In the administration interface, connect to EFT and click the **Server**tab.
2. Do one of the following:
    - On the **Server**tab, click the user account that you want to configure, then in the right pane, on the account's **Connections**tab, select the **AS2 outbound**check box, and then click **AS2 Outbound**. The **AS2 Outbound Settings** dialog box appears.

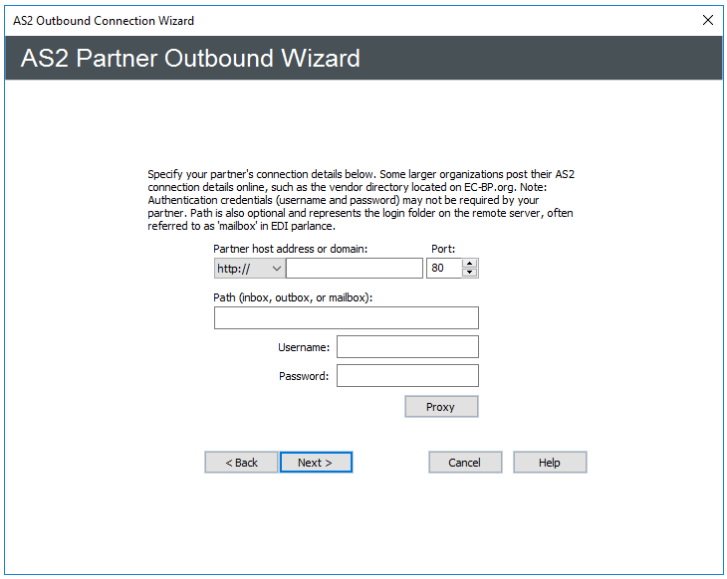


- In an Event Rule, after adding the **AS2 send file to host**action to a Rule, in the Rule Builder, click **select**. The **AS2 Send File** dialog box appears.

3. In either the **AS2 Outbound Settings**dialog box or **AS2 Send File**dialog box, click **Setup Wizard**. The **AS2 Partner Outbound Wizard**appears.

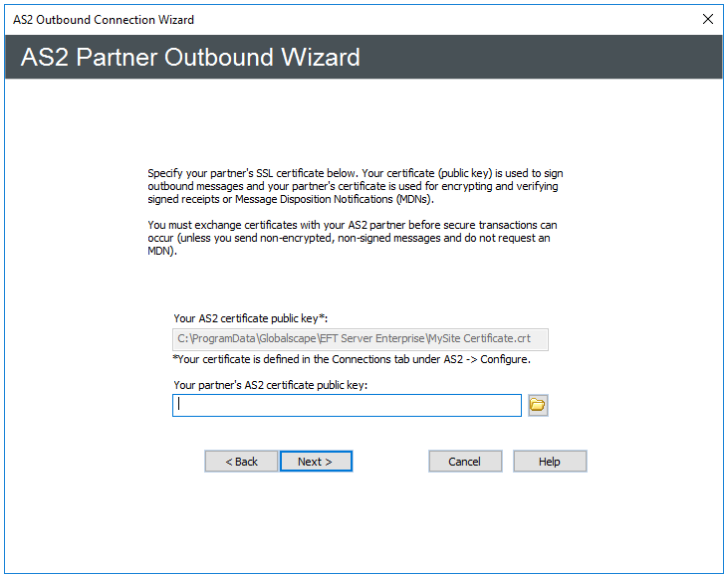


4. Click **Next**. The AS2 partner connection information page appears.



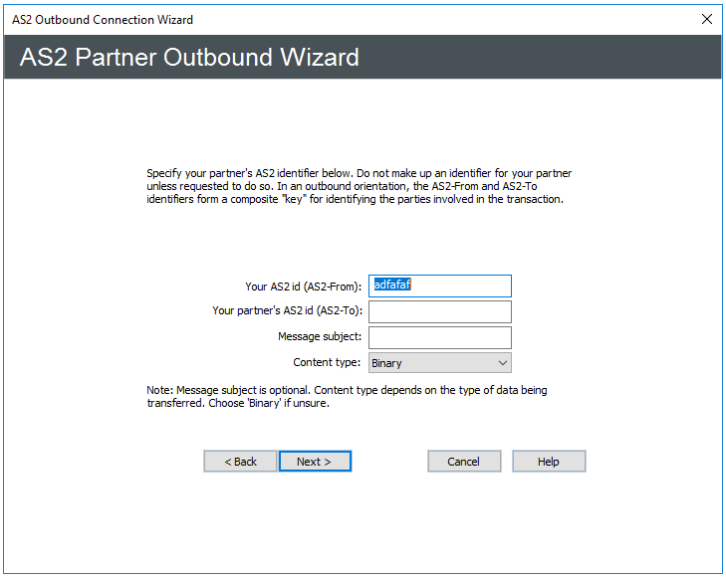
   a. In the **Partner host address or domain** area specify the protocol to use (http:// or https://), IP address/domain name, and **Port**number used to connect to the AS2 partner.
   b. In the **Path**area, provide the path to the inbox, outbox, or mailbox at the AS2 partner location.
   c. In the **Username**and **Password** boxes, provide the logon credentials.
   d. If you need to configure a proxy server, click **Proxy** and then refer to Configuring an AS2 Outbound Proxy for the procedure, if necessary.

5. Click **Next**. The AS2 certificates page appears.



a. In the **Your AS2 certificate public key** box, the certificate that you specified when you created the Site appears.
b. In the **Your partner's AS2 certificate public key** box, type the path or click the folder icon to select your partner's public key file.

6. Click **Next**. The AS2 identifier page appears.

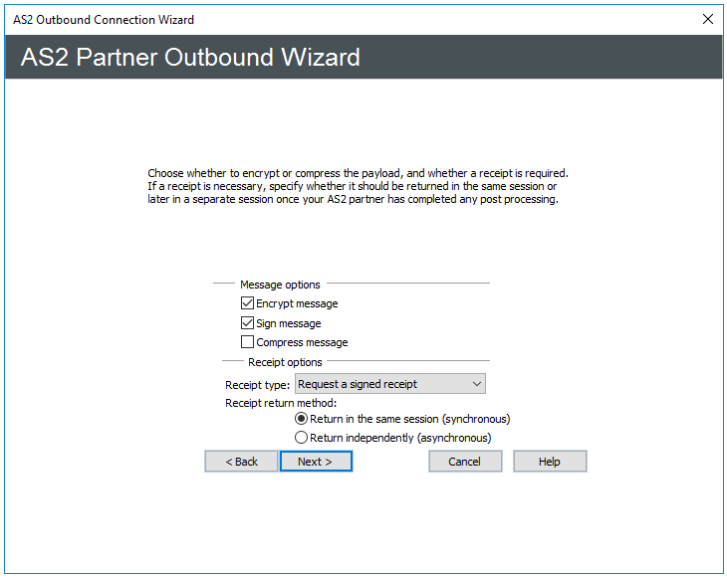


a. In the **Your AS2 ID (AS2-From)** box, your globally defined ID appears. You can use the same ID you defined for EFT when you enabled the AS2 inbound listener or you can define a different ID for each partner.
b. In the **Your partner's AS2 ID (AS2-To)** box, specify this partner's ID (provided to you by the partner that you are defining). **AS2-From**and **AS2-To** form a pair for identifying the sending and receiving partnership. That is, they form a composite key for identifying the parties involved in the data exchange.
c. (Optional) In the **Message subject** box, specify the text that is to appear in the subject line of AS2 messages to/from this partner.
d. In the **Content type** box, click the list to specify the type of messages to be sent to/from this partner.
    - **X12**- Format used by many healthcare, insurance, government, transportation, and finance organizations.
    - **EDIFACT**- Format adopted by the International Organization for Standardization (ISO) as the ISO standard ISO 9735.
    - **XML**- File format used for structured documents.
    - **EDI Consent**- Provides a standard mechanism for "wrapping" the EDI objects but does not specify any details about those objects.

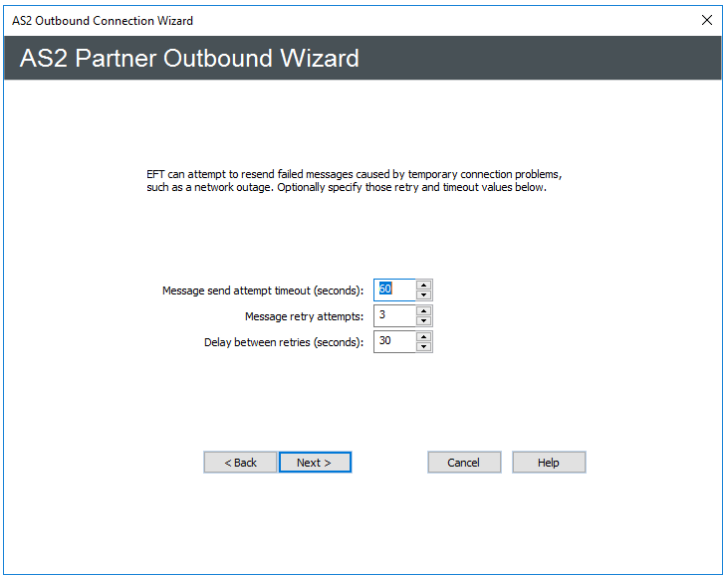
- **Binary**(default) - e.g., executables, word processing files, database, spreadsheet, and multimedia files
- **Plaintext**- e.g., text and HTML files

For information about the various content types, refer to RFC 2046 at http://www.ietf.org/rfc/rfc2046.txt.

7. Click **Next**. The message and receipt options page appears. The MDN serves as a receipt, guaranteeing the transaction was successful.

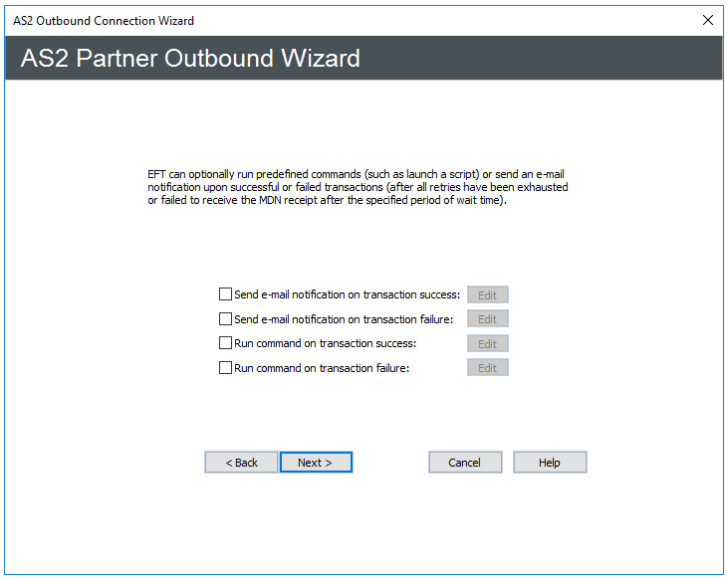


   a. In the **Message options** area, select or clear the check boxes depending on whether the AS2 message should be encrypted, signed, and/or compressed.
   b. In the **Receipt options** area, click the list to specify whether to send a **Request a signed receipt**, **Request an unsigned receipt**,**or Don't request a receipt**.
      - If you clicked **Request a signed receipt** or **Request an unsigned receipt** (not **Don't request a receipt**), specify whether to send the receipt in the same session (synchronous) or independently of the session (asynchronous). Asynchronous receipts will be returned to the domain name specified on the Site's Connection tab using the port specified on that same page.
8. Click **Next**. The message retry and timeout options page appears.



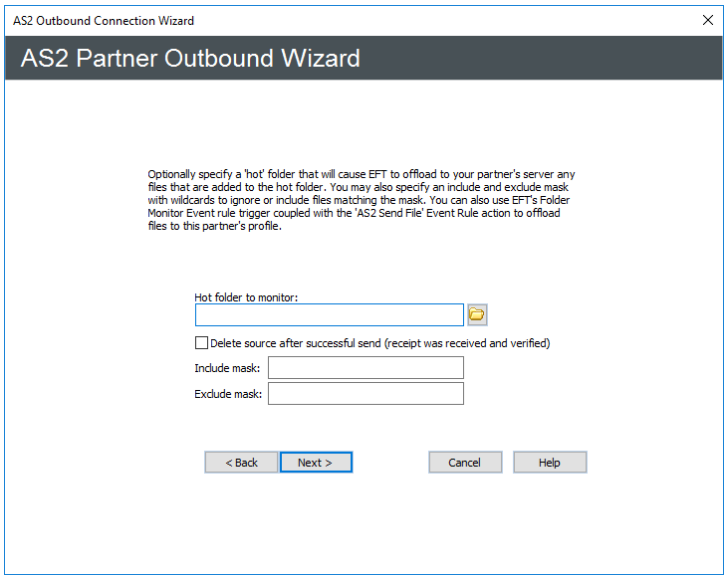
- (Optional) EFT can attempt to resubmit failed messages in case of network outage or other temporary (transitive) errors. EFT will resend the same message, payload, and AS2 Message ID. Specify the following retry and timeout values as needed:
  - **Message send attempt timeout** (seconds). This is the message connection/send timeout. The range is 0-600; 0 = no timeout; the default value = 60 seconds.
  - **Message retry attempts**. The range is 0-9999; (0 = no retry); the default value = 3 retries.
  - **Delay between retries** (seconds). The range is 0-9999; (0 = no wait); the default value = 30 seconds.
  - **Asynchronous receipt timeout** (minutes). The range is 0-999,999; (0 = no timeout); the default value = 7200 minutes (5 days). (This option does not appear if you specified to return the receipt independently/synchronous on the previous page.)

9. Click **Next**. If you define the connection from the user account's **Connection**tab, the transaction success or failure options appear. (This page does not appear in the Event Rule Action configuration.)



- (Optional) Specify whether to send an email notification upon transaction success and/or failure and whether to run a command upon transaction success and/or failure. Select the applicable check box, and then click **Edit**to configure the email or Command.

10. Click **Next**. The hot folder page appears. If you define the connection from the user account's **Connection**tab, the "hot folder" options appear. (This page does not appear in the Event Rule Action configuration.)

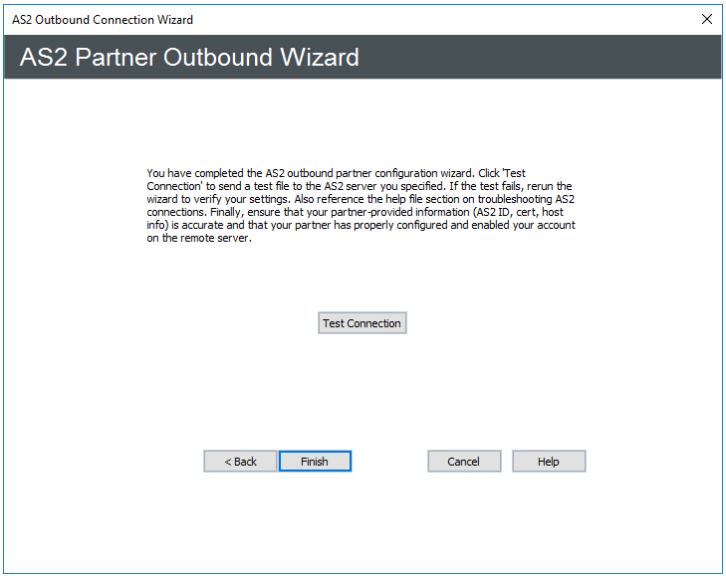


11. Specifying a folder to monitor is optional. If you specify a folder to monitor, EFT will automatically offload to your partner's AS2 server any files that are added to the specified folder. You can offload all files in the folder or only specific files or types of files. Wildcard masks can be used in the **Include mask** and

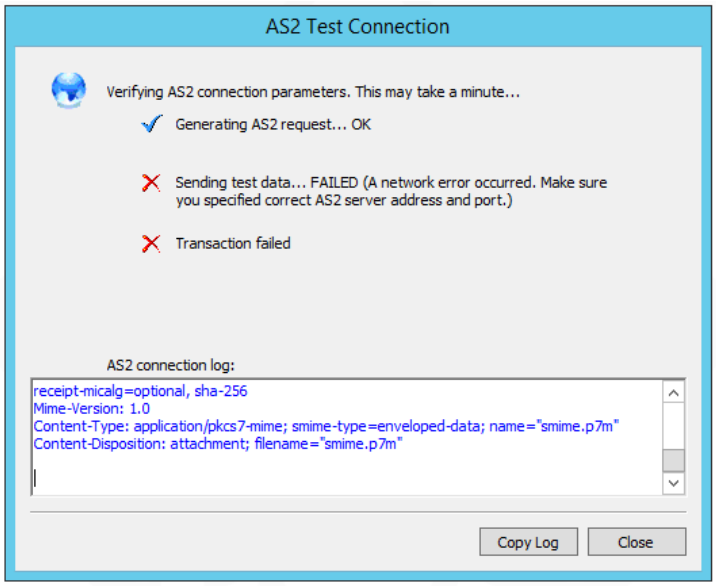
Exclude maskboxes.

- Click the folder icon to specify a folder or type a path in the **Hot folder to monitor**box.
- If you want to delete the source file(s) after they are successfully sent, select the **Delete**check box.
- If you want to specify only certain files are sent, specify the files to include or exclude in the **Include mask** and **Exclude mask**boxes. For example, to exclude all **.wav**files, type ***.wav** in the **Exclude** box. By default, all files are sent (Include mask = ***.***).

12. Click **Next**. The **Test Connection** page appears.



a. Click **Test Connection**. The **AS2 Test Connection**dialog box appears.



b. EFT attempts to connect to the AS2 partner and send test data.
   - If the test fails, data appears in the AS2 connection log area that you can copy to the clipboard to be pasted in a text file or email for troubleshooting. Click **Close**, then in the wizard click **Back**to adjust settings, if necessary.
   - If the test is successful, click **Close**.

13. Click **Finish**. The information provided in the wizard is updated in the account's **AS2 Outbound** tab. To make further adjustments to the partner's configuration, you can edit the AS2 Outbound tab directly.

Configuring AS2 Inbound Partners Using the Wizard

(Requires AS2 and HTTP/S module) EFT provides an **AS2 Partner Access** wizard to assist you in configuring AS2 inbound connections. This wizard is accessible from the **AS2 Inbound** partner configuration tab and the **AS2 Send File to host Action** dialog box (in Event Rules). Once completed, the data in the wizard populates the relevant fields on the **AS2 Inbound** tab and the **AS2 Send File to host Action** dialog box. The procedure below describes how to use the wizard to configure inbound AS2 partners. You can also configure the account manually on the **AS2 Inbound** tab for each partner.

Before you start the wizard to configure inbound AS2 partners, you will need to request the following information from your partner:

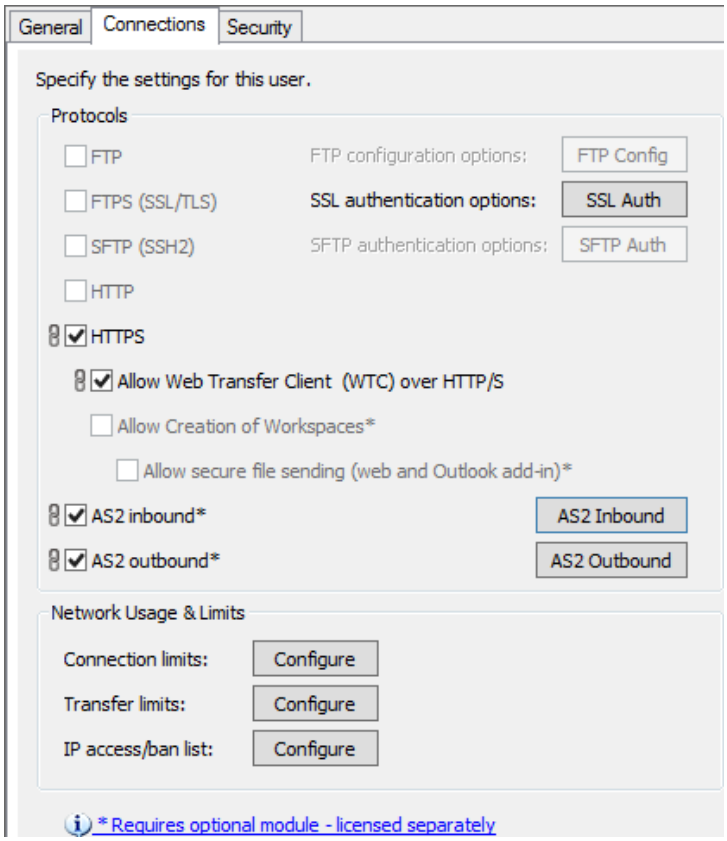
- AS2 identifier
- SSL certificate (public key file)

If you plan to execute a command upon success or failure of AS2 transactions, define the command before configuring your partner access; or you can go back later and edit the AS2 partner manually after you have defined the command.

If you plan to send a notification email upon success or failure of AS2 transactions, you can Create an email Notification Template to use in the email Action.

To configure inbound AS2 partners using the wizard

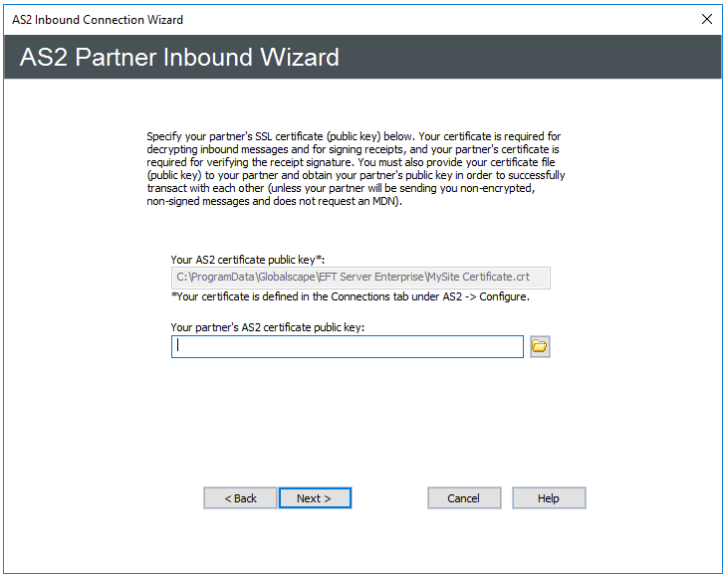
1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the *user account* that you want to configure. This account is one that your partner uses to exchange EDI messages with you.
3. In the right pane, click the **Connections** tab.



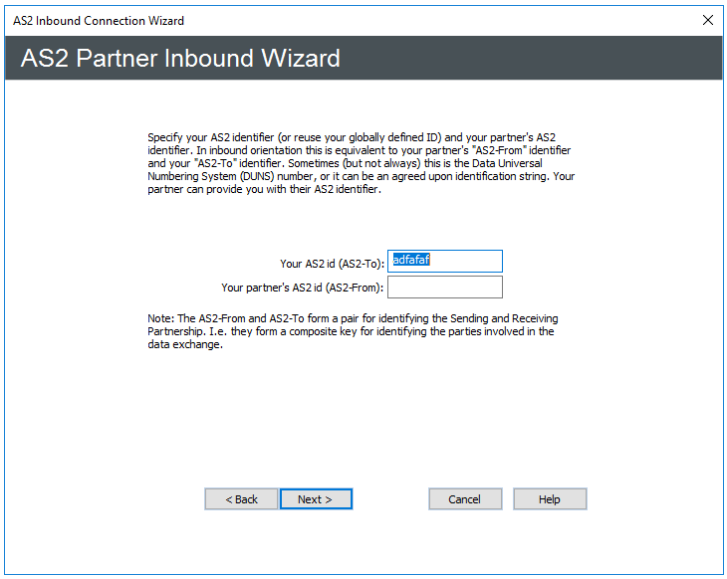
If the AS2 features are not available for the user, then AS2 is disabled on the Settings Template or the Site. Enable and configure AS2 on the Site before enabling AS2 on the Settings Template and user accounts.

4. Select the **AS2 inbound** check box and then click **AS2 Inbound**. The **AS2 Inbound Settings** dialog box appears.
5. Click **Setup Wizard**. The **AS2 Partner Inbound Wizard** appears.

6. Click **Next**. The AS2 certificates page appears.



   a. In the **Your AS2 certificate public key** box, the certificate that you specified when you created the Site appears.
   b. In the **Your partner's AS2 certificate public key** box, type the path or click the folder icon to select your partner's public key file.
7. Click **Next**. The AS2 identifier page appears.

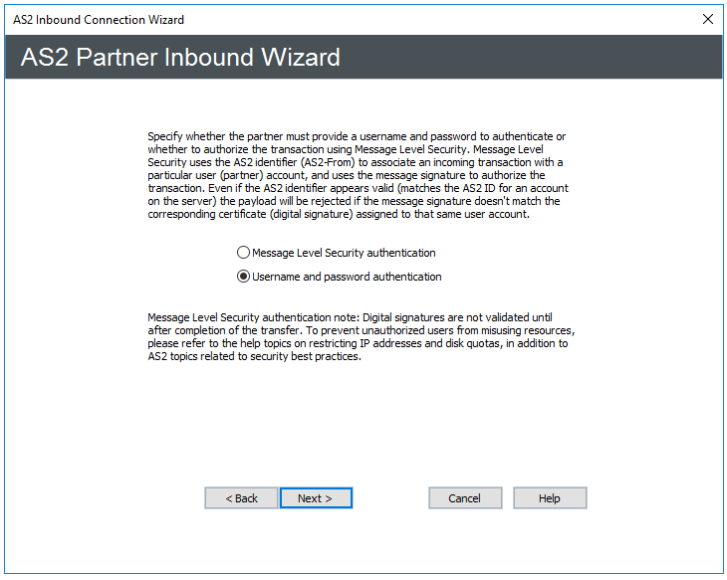


a. In the **Your AS2 ID (AS2-To)** box, your globally defined ID appears. You can use the same ID you defined for EFT when you enabled the AS2 inbound listener or you can define a different ID for each partner.

b. In the **Your partner's AS2 ID (AS2-From)** box, specify this partner's ID (provided to you by the partner that you are defining).

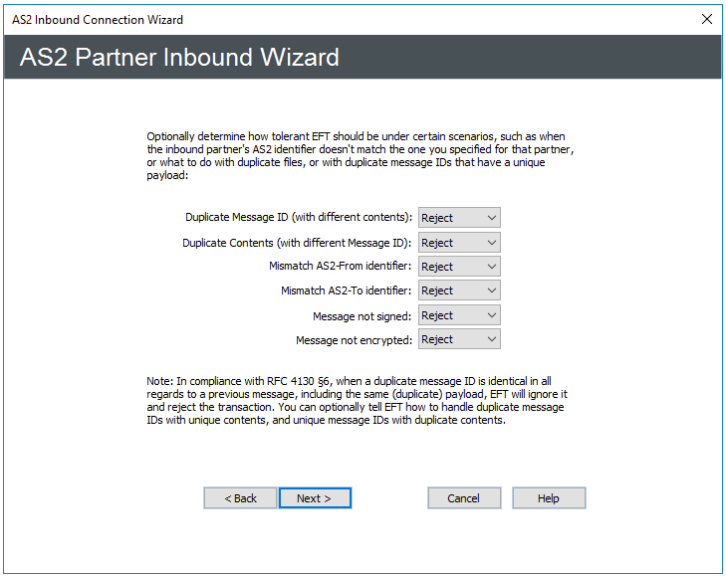
   AS2-From and **AS2-To** form a pair for identifying the sending and receiving partnership. That is, they form a composite key for identifying the parties involved in the data exchange.

8. Click **Next**. The authentication page appears.



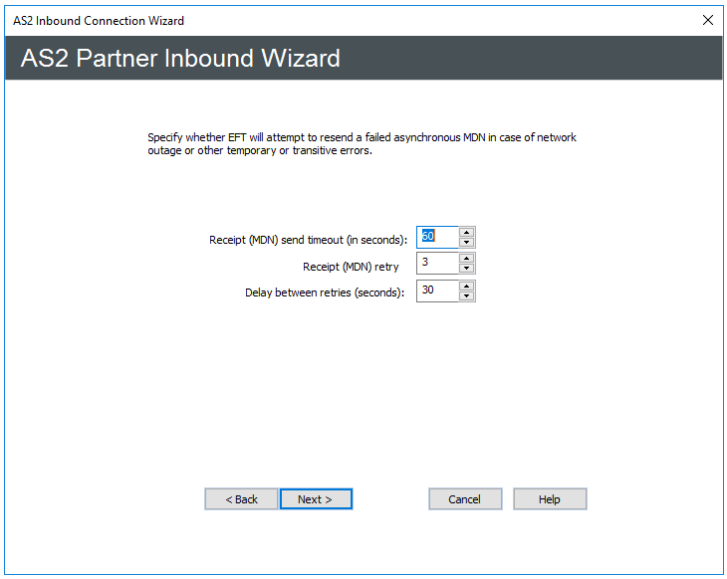
- Specify whether this partner must provide a username and password to connect or if EFT will authorize transactions from this partner using Message Level Security.

9. Click **Next**. The tolerance options page appears.

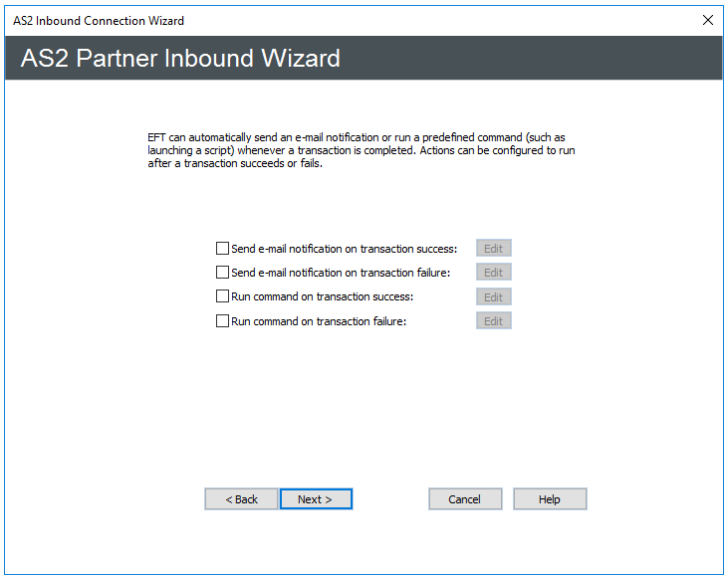


- (Optional) When a duplicate message ID is identical in all regards to a previous message, including a duplicate payload, EFT will ignore it and reject the transaction. You can tell EFT to accept or reject duplicate message IDs with unique contents, unique message IDs with duplicate contents, and mismatched AS2-From or AS2-To identifiers. For each option, the default is to reject the transaction. If you specified Message-Level Security (MLS) authentication on the previous page, the **Mismatch AS2-From** identifier and **Message not signed** options cannot be changed. Specify whether to **Accept** or **Reject** messages for each of the following instances:
  - **Duplicate Message ID** (with different contents)
  - **Duplicate content** (with different Message ID)
  - **Mismatch AS2-From identifier** (cannot change to Accept for MLS authentication)
  - **Mismatch AS2-To identifier**
  - **Message not signed** (cannot change to Accept for MLS authentication)
  - **Message not encrypted**

10. Click **Next**. The resend options page appears.



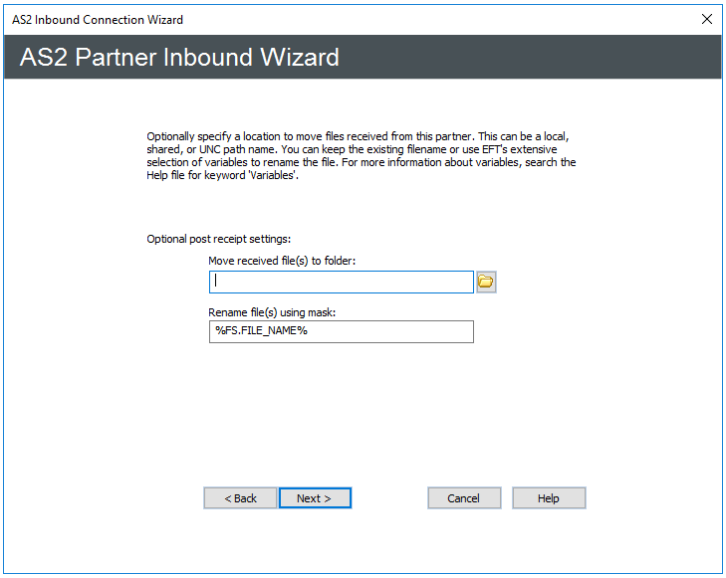
11. Specify whether EFT will attempt to resend failed asynchronous MDN in case of network outage or other temporary (transitive) errors.
    - **Receipt (MDN) send timeout** (seconds). Range: 0-600; (0 = no timeout); the default value = 60 seconds
    - **Receipt (MDN) retry**. Range: 0-999; (0 = no retry); the default value = 3 retries.
    - **Delay between retries (seconds)**. Range: 0-600; (0 = no wait); the default value = 30 seconds.
12. Click **Next**. The commands and notifications page appears.



- (Optional) EFT can run predefined commands (such as launch a script) or send an email notification upon successful or failed transactions (after all retries have been exhausted or failed to receive the MDN receipt after the specified wait time). Select one or more of the following check boxes, then click **Edit** to configure the email notification or specify the Command to use.
  - Send email notification on transaction success
  - Send email notification on transaction failure
  - Run command on transaction success
  - Run command on transaction failure

  Refer to AS2 Transaction Success and Failure Notifications for more information.

13. Click **Next**. The optional post receipts page appears.



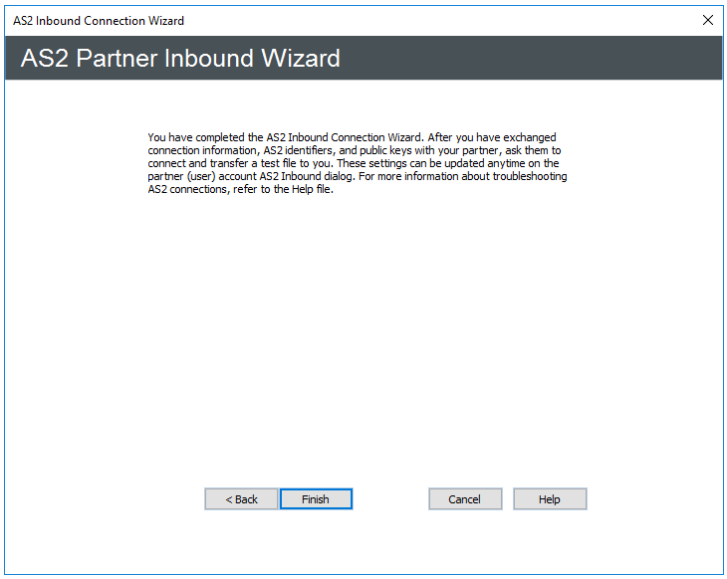
- (Optional) In the **Move received file(s) to folder** box, specify a location to move received files, including local, shared, or UNC path names. (Leave blank to not move the file.)
- In the **Rename file(s) using mask** box, provide a name for the file, if you want to change it. (The variable `%FS.FILE_NAME%` appears in the box by default.)

  You can keep the existing filename or use EFT's extensive variable selection to rename the file, and add pre- or post-pending dates, times, and other information. For example, if you want to add the date and

time to the filename, you would provide the following variables in the **Rename file(s) using mask** box:

%FS.FILE_NAME%_%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%

14. Click **Next**. Configuration is complete.

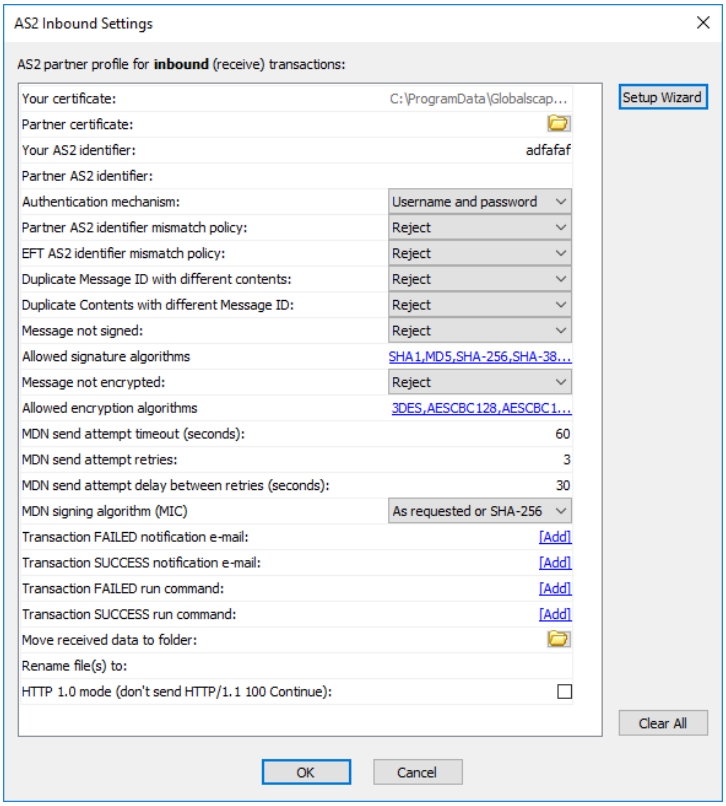


15. Click **Finish**. Now that you have completed the AS2 inbound partner configuration wizard, you should contact your partner and ask them to connect and transfer a test file. Refer to Troubleshooting AS2 Connections for details.

The information provided in the wizard is updated in the account's **AS2 Inbound** tab. To make further adjustments to the partner's configuration, you can edit the AS2 Inbound tab directly.

AS2 Inbound Parameters

(Requires AS2 and HTTP/S module) For AS2 inbound (receiver) connections for transactions over the HTTP and HTTPS ports, enable AS2 by selecting the **AS2**check box on the Site's **Connections**tab. You can enable or disable AS2 for partner (user) accounts on the Settings Template and/or for each user, or by selecting AS2 in the **New User Creation** wizard on the protocol selection page when you create the partner account. The standard inheritance rules apply. (AS2 has to be enabled and configured for the Site before you can enable it for a Settings Template or user account.)



The parameters in the table below are available in the **AS2 Inbound Settings** dialog box and can be configured manually or using the setup wizard.

- Click **Setup Wizard**to Configure AS2 Inbound Partners Using the Wizard.
- Click **Clear All**to reset all of the fields to default values. (A confirmation prompt appears.)

Parameter	Required/Optional	Description
Your certificate	Required	Displays the AS2 certificate public key path to be used for signing the MDN and for decryption, copied from the Site. (Can be on a drive or UNC path.)

Parameter	Required/Optional	Description
Partner certificate	Required	Specifies the AS2 certificate to be used for verifying signed messages. (Can be on a drive or UNC path.)
Your AS2 identifier	Required	Your AS2 identifier.
Partner AS2 identifier	Required	Your partner's AS2 identifier (must be unique)
Authentication mechanism	Required	Used to specify whether the client is authenticating with username and password or using Message Level Security (MLS). Refer to AS2 Authentication for more information.
Partner AS2 identifier mismatch policy	Required	Used to accept or reject AS2 transactions where the connecting partner's **AS2-From**ID does not match the AS2 identifier defined for that partner. • Reject (default) - Disallow the transaction • Accept - Allow the transaction
EFT AS2 identifier mismatch policy	Required	Used to accept or reject AS2 transactions where the connecting partner's **AS2-To**ID does not match EFT AS2 identifier defined for that partner in that partner's **AS2Inbound** tab. • Reject (default) - Disallow the transaction • Accept - Allow the transaction
Duplicate Message ID with different contents (For duplicate message ID with same contents, refer to Troubleshooting AS2 Issues.)	Required	Used to Accept or Reject AS2 transactions with duplicate Message IDs. • If an incoming request has the same Message ID and the same payload as a prior incoming message, EFT sends the exact same response from that prior transaction back to the client, and does not extract or process the payload (that is, discards the payload, does not save to file system, does not trigger Event Rules, etc.). • If an incoming request has the same Message ID, but the payload is different, EFT processes or discards the message based on the configuration provided by the user. Options include: • Reject (default) - Disallow the transaction • Accept - Allow the transaction

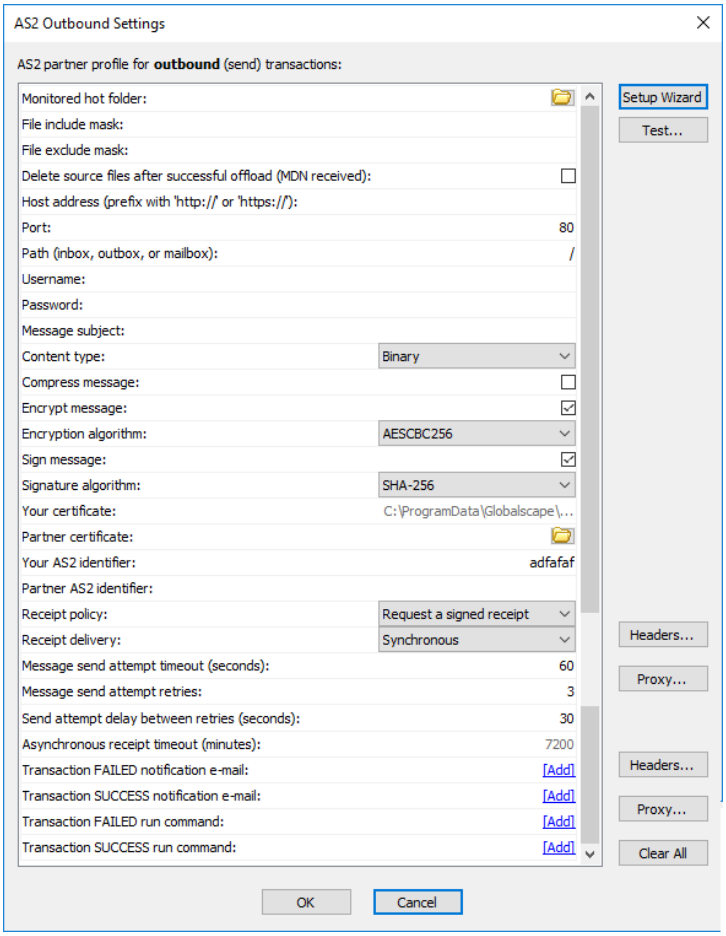
Parameter	Required/Optional	Description
Duplicate Contents with different Message ID	Required	Used to overwrite or reject AS2 transactions where the file is a duplicate of an existing file already residing in the upload directory. • Reject (default) - Disallow the transaction • Overwrite - Overwrite the existing file with the new version • Numerate - Add a unique number to the filename
Message not signed	Required	Used to specify whether EFT will Accept or Reject the transaction if it is not signed.
Allowed signature algorithms	Optional	Used to allow or not allow specific signature algorithms.
Message not encrypted	Required	Used to specify whether EFT will Accept or Reject the transaction if it is not encrypted.
Allowed encryption algorithms	Optional	Used to allow or not allow specific encryption algorithms.
MDN send attempt timeout (seconds)	Required	Specifies the timeout period after which an asynchronous MDN send attempt shall be considered a failure if no response is received from the remote server. Range: 0-600, 60 seconds is the default. 0 = no timeout. Asynchronous receipts will be returned to the domain name specified on the Site's **Connection**tab using the standard or secure listener port specified on that same page (depending on whether you specified HTTP or HTTPS for the remote host value).
MDN send attempt retries	Optional	Number of time to attempt to send MDN. Range: 0 (no retry) to 999; 10 is the default. Retries do not include the initial attempt. That is, 10 retries means 10 in addition to the first attempt (11 total).
MDN send attempt delay between retries (seconds)	Optional	Retry interval. Range: 0 (no wait) to - 600 seconds; 30 seconds is the default. Failure only occurs after all attempts to send MDN have failed. Likewise, success is only after complete transaction has occurred (file received and MDN is sent).
MDN signing algorithm	Optional	Used to specify the MDN signing algorithm. The default is "as requested or SHA-256.
Transaction FAILED notification email*	Optional	Opens the **Edit Mail Template** in which you can specify an email notification for failed transaction. (Refer to email Notification Action for details of defining an email notification.)

Parameter	Required/Optional	Description
Transaction SUCCESS notification email*	Optional	Opens the **Edit Mail Template** in which you can specify an email notification for successful transaction. (Refer to email Notification Action for details of defining an email notification.)
Transaction FAILED run command*	Optional	Opens the **Custom Command** dialog box in which you can specify a Custom Command to occur upon failed send. (Refer to Creating a Command to create a command and refer to Script: Custom Command Action for details of using a Command.)
Transaction SUCCESS run command*	Optional	Opens the **Custom Command** dialog box in which you can specify a **Custom Command** to occur upon successful run. (Refer to Creating a Command to create a command and refer to Script: Custom Command Action for details of using a Command.)
Move received data to folder	Optional	Specify a folder in which to save received data. (Can be on a drive or UNC path.)
Rename file(s) to	Optional	Appends filename to path using specified variables. Preserve filename if undefined. This parameter is the same as the Specify relative path and filename field in the **Target File** tab of the **Offload Action**wizard in EFT's Copy/Move File to Host Action.
HTTP 1.0 mode (don't send HTTP/1.1 100 Continue)	Optional	"100 Continue" is a part of the HTTP protocol and means "Everything is OK for now, continue this transaction"; many AS2 servers use it to avoid timeouts. It is the client software's responsibility to process this reply properly (just skip until 200 OK or real HTTP error is received); if the client does not process the reply correctly, you can turn off the "100 Continue" response by selecting the check box. (The check box is cleared by default.) If your AS2 partner receives multiple MDN failures when sending to EFT in HTTPS, select this check box to turn off the "100 Continue" reply.

***** EFT sends emails and executes commands only after the final transaction status (Failure or Success) is known.

AS2 Outbound (Sender) Parameters

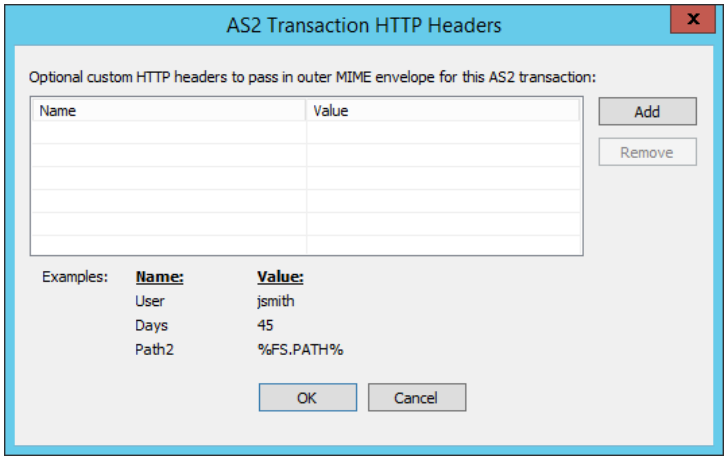
(Requires AS2 and HTTP/S module) For AS2 outbound (sender) connections for transactions over the HTTP and HTTPS ports, enable AS2 by selecting the **AS2**check box on the Site's **Connections**tab. You can enable or disable AS2 in the Settings Template and/or for the user account, or by selecting AS2 in the **New User Creation** wizard on the protocol selection page when you create the user. The standard AS2 Outbound (Sender) Parameters rules apply. (AS2 has to be enabled and configured for the Site before you can enable it for a Settings Template or user account.)



The parameters in the table below are available in the **AS2 Outbound Settings** dialog box can be configured manually or using the setup wizard.

- Click **Setup Wizard**to Configure AS2 Outbound Partners Using the Wizard.
- Click **Test** to Test the connection to the partner.

- (Optional) Click **Headers**to add a custom header. The purpose of custom HTTP headers is to pass additional or required information to the recipient's server. The **Name** and **Value**fields can each contain up to 255 characters. The Value fields can use AS2 Outbound (Sender) Parameters



  - To add the header, click **Add**, then provide the name and value in the table, as shown in the examples in the dialog box.
- Click **Proxy**to launch the **Proxy Settings** dialog box. You can forward the connection through the DMZ Gateway (as a SOCKS5 proxy) or an HTTP proxy of your choosing.
- Click **Clear All**to reset all of the fields to default values. (A confirmation prompt appears.)

Parameter	Required/Optional	Description
Monitored hot folder	Optional	Specifies the monitored folder for added files. If no folder is specified, no folder monitoring occurs. The partner profile can be invoked from the Event Rules. (Can be on a drive or UNC path.)
File include mask	Optional	Used to include files based on their extension for sending to the destination to the partner's remote AS2 host. For example, include only **.txt**files. Defaults to asterisk (*) to include all files. Blank also means include all files. Accepts wildcard masks; semicolon or comma delimited.
File exclude mask	Optional	Used to exclude files based on their extension from sending to the destination to the partner's remote AS2 host. For example, exclude **.txt**files. Defaults to blank, which means exclude no files. Accepts wildcard masks, semicolon or comma delimited.

Parameter	Required/Optional	Description
Delete source after successful offload (MDN received)	Required	Used to delete sources files after sending them to the destination, after the MDN is received and verified from the remote AS2 host. Selected by default.
Host address	Required	AS2 Outbound host address. Requires protocol prefix in URL (http:// or https://). Specified in **AS2 Partner Access** wizard.
Port	Required	AS2 Outbound port. Range is 1-65K; defaults to 80 if host address is preceded by http; 443 if host address is preceded by https.
Path	Optional	Relative path to the remote directory, such as, **/partnerXYZ**, **/partners/mailboxes/xyz**, or **/192.168.20.16/path**
Username	Optional	User login name
Password	Optional	Password
Message subject	Optional	AS2 message subject
Content type	Required	AS2 content type. Options include: • **X12**- Format used by many healthcare, insurance, government, transportation, and finance organizations. • **EDIFACT** - Format adopted by the International Organization for Standardization (ISO) as the ISO standard ISO 9735. • **XML** - File format used for structured documents. • **EDI Consent** - Provides a standard mechanism for "wrapping" the EDI objects but does not specify any details about those objects. • **Binary** (default) - e.g., executables, word processing files, database, spreadsheet, and multimedia files • **Plaintext** - e.g., text and HTML files • For information about the various content types, refer to RFC 2046 at http://www.ietf.org/rfc/rfc2046.txt.
Compress message	Required	When selected, specifies that the AS2 message should be compressed when sent. (Cleared by default.)
Encrypt message	Required	When selected, specifies that outbound AS2 messages should be encrypted. (Selected by default.)
Encryption algorithm	Optional	Used to specify the encryption algorithm to use for outbound transactions. AESCBC256 is used by default.
Sign message	Required	When selected, specifies that outbound AS2 messages should be signed. (Selected by default.)

Parameter	Required/Optional	Description
Signature algorithm	Optional	Used to specify the signature algorithm to use for outbound transactions. SHA-256 is used by default.
Your certificate	Required	Displays the AS2 certificate public key path to use for signing, copied from the Site. (Can be on a drive or UNC path.)
Partner certificate	Required	Specifies the AS2 certificate to use for encrypting outbound transactions and for validating signed MDN receipts. (Can be on a drive or UNC path.)
Your AS2 identifier	Required	Used to apply a unique **AS2-From**ID to outbound messages.
Partner AS2 identifier	Required	Used to apply a unique **AS2-To**ID to outbound messages.
Receipt policy	Required	Used to request an MDN receipt. Options include: • Don't request a receipt • Request a signed receipt (default) • Request an unsigned receipt
Receipt delivery	Required	Specifies receipt delivery method • Synchronous (default) • Asynchronous (see Asynchronous receipt timeout, below)

The following fields are used to determine whether a message send attempt has failed due to a timeout, error, or synchronous MDN receipt failure, or other error, after which EFT will attempt to resend the same message at regular intervals, if specified. Because EFT is sending the same content, it will resend the same message, payload, and AS2 Message ID.

Parameter	Required/ Optional	Description
Message send attempt timeout (seconds)	Optional	Specifies the timeout after which a message send attempt is considered a failure if no response or error is received from the remote server. Range: 1-99999 seconds; 60 by default. A value of 0 is not accepted.
Message send attempt retries	Optional	Number of times to reattempt to send the message. Range: 0 (no retry) to 999, 10 is the default. Retries do not include the initial attempt. That is, 10 retries means 10 in addition to the first attempt (11 total).
Send attempt delay between retries	Optional	Interval between resend attempts. Range: 0 (no wait) to - 600 seconds; 30 seconds is the default

Parameter	Required/ Optional	Description
Asynchronous receipt timeout	Optional	Specifies the timeout after which EFT determines whether an asynchronous receipt was received. Range: 0 (no timeout) to 999,999 minutes; 7200 minutes (5 days) is the default. If the MDN is received after the timeout expires, the MDN is discarded, EFT returns an HTTP error code to the sender, and triggers the transaction failure event, if defined.
Transaction FAILED notification email*	Optional	Opens the **Edit Mail Template** in which you can specify an email notification for failed transaction. (Refer to email Notification Action for details of defining an email notification.)
Transaction SUCCESS notification email*	Optional	Opens the **Edit Mail Template** in which you can specify an email notification for successful transaction. (Refer to email Notification Action for details of defining an email notification.)
Transaction FAILED run command*	Optional	Opens the **Custom Command** dialog box in which you can specify a Custom Command to occur upon failed send. (Refer to Creating a Command to create a command and refer to Script: Custom Command Action for details of using a Command.)
Transaction SUCCESS run command*	Optional	Opens the **Custom Command** dialog box in which you can specify a Custom Command to occur upon successful send. (Refer to Creating a Command to create a command and refer to Script: Custom Command Action for details of using a Command.)

***** EFT sends emails and executes commands only after the final transaction status (Failure or Success) is known.

Configuring an AS2 Outbound Proxy

(Requires AS2 and HTTP/S module) If you need to configure a proxy server for outbound AS2 transmissions, the option is available on the **AS2 Outbound** tab.

To configure an outbound proxy

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the user (trading partner) you want to configure.
3. In the right pane, click the **Connections** tab.
4. Click **AS2 Outbound**. The **AS2 Outbound Settings** dialog box appears.
5. Click **Proxy**. The **Proxy Settings** dialog box appears.
6. Select the **Use proxy settings below when connecting to remote host** check box. The **Proxy type** options become available.
7. Click one of the following:
   - **Use EFT's DMZ Gateway as the proxy** to use DMZ Gateway as a SOCKS5 proxy.
   - **HTTP proxy** to use another proxy via HTTP, and specify the **Host name**, **Port**, **Username**, and **Password**.
8. Click **OK** to save the settings and return to the **AS2 Outbound** tab.
9. Click **Apply**.

Initiating AS2 Outbound Transactions

(Requires AS2 and HTTP/S module) EFT's AS2 module provides the ability to initiate outbound AS2 transactions as an AS2 client; that is, an *AS2 Sender.* The Server provides two methods for initiating AS2 outbound transactions, described below:

- **Partner Profile method**. A Folder Monitor Event trigger mapped directly to a user account's (trading partner's) AS2 profile can monitor a specified folder for files added and, when triggered, send those files to the specified partner AS2 profile. This Event is neither visible nor editable in the **Event Rules** node.
- **Event Rules**. The AS2 Send file to host Event Rule Action can be triggered using the Scheduler (Timer) Event, Folder Monitor Event, or any file-based Event trigger. When triggered, the AS2 Send file to host Action uses the provided configuration data to send the context or manually specified file(s) to the specified partner AS2 profile. (Refer to Sending Files to an AS2 Partner via Event Rules for details.)

To use the Partner Profile method

1. In the administration interface, connect to EFT and click the **Server** tab.
2. Configure a reusable AS2 partner profile. (Create a new user or modify an existing user account.)
3. In the left pane, click the user (trading partner) you want to configure.
4. In the right pane, click the **Connections** tab.
5. Click **AS2 Outbound**. The **AS2 Outbound Settings** dialog box appears.
6. In the **Monitored hot folder** box, click the open icon to specify a folder that is tied to that partner profile/user account (for example, the user's Home folder).
7. Click **OK** to close the **Browse for Folder** dialog box.
8. Click **OK** to close the **AS2 Outbound Settings** dialog box.
9. Click **Apply** to save the changes on EFT.

EFT verifies whether the selected folder exists and, if not, displays an error message. If a file is added to the hot folder, it is immediately sent to the predefined remote AS2 host and (optionally) deleted from the source location after a confirmed send (MDN received and verified). This method creates a hidden Folder Monitor Event Rule with an "If user is" Conditional statement that triggers an AS2 Send File to host Action when files are added to the folder.

Refer to the "Event Rules User Guide" for details of using AS2 Actions.

Moving Files Received from AS2 Partners

You can configure AS2 inbound transfers to move and/or rename files after they are received. These settings, combined with setting **Duplicate Contents with different Message ID** to **Reject** will prevent received files of the same name and extension from being overwritten.

To move received files

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the user (trading partner) you want to configure.
3. In the right pane, click the **Connections** tab.
4. Click **AS2 Inbound**. The **AS2 Inbound Settings** dialog box appears.
5. To specify the folder in which to move all received files, in the **Move received data to folder** box, click the folder icon. The **Browse for folder** dialog box appears.
6. Click a folder or click **Make New Folder** to create a new folder, and then click **OK**. The folder path appears in the **Move received data to folder** box.
7. Click **OK** to close the **AS2 Inbound Settings** dialog box.
8. Click **Apply** to save the changes on EFT.

Related Topics

- Configuring AS2 Inbound Partners Using the Wizard
- Renaming Files Received from AS2 Partners

Renaming Files Received from AS2 Partners

You can configure AS2 inbound transfers to moveand/or rename files after they are received. These settings, combined with setting **Duplicate Contents with different Message ID** to **Reject** will prevent received files of the same name and extension from being overwritten.

To rename received files

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the user (trading partner) you want to configure.
3. In the right pane, click the **Connections**tab.
4. Click **AS2 Inbound**. The **AS2 Inbound Settings** dialog box appears.
5. In the **Rename file(s) to** box, click in the far right to activate the text box, then provide the characters and/or variables with which to change the name of received files. Use `%EVENT.DATESTAMP%`and `%EVENT.TIMESTAMP%`to add the date and time to the file name. Use `%FS.FILE_NAME%`for the name of the file.

   For example, if you type:

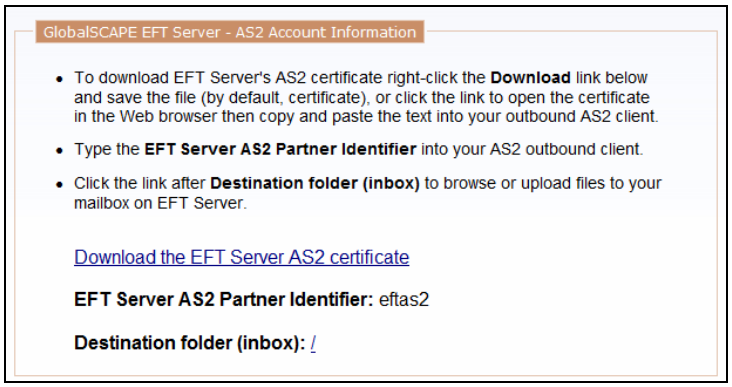
   `%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%_%FS.FILE_NAME%`

   A file transferred as `dailyprogress.doc` on May 3, 2008 at 10:56:26 would be renamed to `05032008_105626_dailyprogress.doc`.
6. Click **OK** to close the AS2 Inbound Settings dialog box.
7. Click **Apply**to save the changes on EFT.

AS2 Account Information Web Page

(Requires AS2 and HTTP/S module) EFT provides an AS2 Web page at the reserved path of **/as2**. On this page, partners can access the following information:

- EFT's public AS2 certificate (**https://localhost/as2/certificate**)
- The Site's AS2 Global Identifier (Refer to Enabling the AS2 Inbound Listener Service for details of specifying the AS2 ID.)
- The destination folder (inbox/mailbox). (The destination folder is the ***Specifying a Home Folder* on page 1039**, configured on the **General** tab of the partner/user account.)



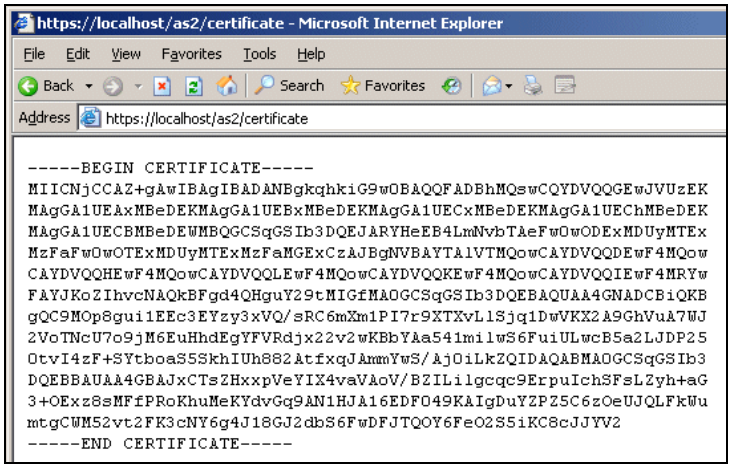
Your trading partners can access EFT's AS2 certificate from the AS2 Account Information page. Provide your trading partners with the URL of the page (for example, https://mycompanyAS2website/as2), then instruct them as described below. (Instructions are also provided on the Web page.)

To open the AS2 Account Information page

1. Open a browser and go to the URL provided to you by the EFT administrator (for example, https://mycompanyAS2website/as2). A log in page appears.
2. Log in with your EFT credentials. The **AS2 Account Information** page appears.

To download the Server's AS2 certificate

- Do one of the following:
  - Right-click the **Download EFT AS2 certificate** link, click **Save Target As**, specify a location for the certificate, then click **Save**. The file is saved as **certificate.txt**. To use the file for EFT, change the extension to **.crt**.
  - Click the **Download** link. The certificate contents display in the browser.



- Copy and paste the contents of the page into your AS2 application's certificate box. (Include BEGIN CERTIFICATE and END CERTIFICATE.)

Allowing AS2 Connections to a Site

(Requires AS2 and HTTP/S module) AS2 connections must be configured on EFT before you can enable AS2 connections in the Site, Settings Template, or user account.

AS2 is a separately licensed product. It is available during the trial period; however, when EFT trial expires, the AS2 module trial also expires.

To allow AS2 connections to a Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site that you want to configure.
3. In the right pane, click the **Connections**tab.
4. In the **Listener Settings**area, select the **AS2** check box.
5. Click **AS2 Config**. Refer to Enabling the AS2 Inbound Listener Service for details of AS2 configuration.
6. Click **Apply**to save the changes on EFT.

Related Topic

- AS2 Module

Allowing AS2 Connections in the Settings Template or User Account

(Requires AS2 and HTTP/S module) AS2 connections must be configured on the Site before you can enable AS2 connections in the Settings Template or user account.

To allow AS2 connections for Settings Templates or user accounts

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Settings Template or user account that you want to configure.
3. In the right pane, click the ***Connections Tab of a User Account* on page 1013** tab.
4. In the **Protocols** area, select the **AS2** check box.
5. Click **AS2 Inbound** to configure inbound connections; click **AS2 Outbound** to configure outbound connections.
6. Click **Apply** to save the changes on EFT.

Related Topics

- The AS2 Module
- Configuring the AS2 Module
- Troubleshooting AS2 Connections

AS2 Events, Conditions, Actions, and Variables

(Requires AS2 and HTTP/S module) The topics below provide information and procedures for defining Event Rules to automate AS2 transfer activities. For details of defining Event Rules, refer to Creating Event Rules.

- Introduction to AS2 Events Conditions Actions and Variables
- AS2-Related Events
- AS2-Related Conditions
- AS2-Related Actions
- AS2-Related Context Variables

Introduction to AS2 Events, Conditions, Actions, and Variables

AS2 transfers can have more than a simple success or failure outcome. For example, an outbound AS2 file transfer may succeed, but no MDN is received from the remote host. This could be considered an outright failure in some cases. Another example may include a successful file send followed by MDN received, but the received MDN's signature cannot be verified. Some AS2 systems do not consider these failures as an overall failure, but others will. For example, a remote host may accept an inbound file and log that the signature is bad, yet still accept the file. Likewise, EFT by default accepts most AS2 transmissions, even if there is a MIC mismatch or the signature used to sign the payload was not found; however, the overall transaction is not considered a success unless every part of the transmission succeeds.

EFT always rejects inbound unencrypted transmissions over plaintext HTTP protocol, and upload attempts to a folder to which the user has no write permissions. EFT considers these overall permanent failures.

For details of the AS2 Send File Action, refer to Sending Files to an AS2 Partner in the Event Rules chapter.

Refer to the following topics for information about AS2 Events, Conditions, Actions, and Variables:

- AS2 Events
- AS2 Conditions
- AS2 Send File - Sending Files to an AS2 Partner
- AS2 Variables

AS2 Events

(Requires AS2 and ARM) In **AS2 Inbound Transaction Succeeded** and **AS2 Inbound Transaction Failed** Events, the `FS.FILE_NAME` variable contains the name of the file uploaded (for a simple transaction) or an empty string (for a Multiple Attachment (MA) transaction).

- **AS2 Inbound Transaction Succeeded**—Triggers if the inbound transmission was successful, MDN was successfully sent, MICs all match, and no other errors occurred.
- **AS2 Inbound Transaction Failed**—Triggers if the AS2 file upload failed for some reason, such as bad MIC, no permissions/ access, duplicate message ID, or other AS2 transfer-related error.
- **AS2 Outbound Transaction Succeeded**—Triggers if EFT has offloaded a file to a remote partner, and that partner replied with a receipt over HTTP/S, indicating that the transfer was successfully completed.
- **AS2 Outbound Transaction Failed**—Triggers if the expected MDN receipt was not received in the expected time or the receipt signature or MIC failed.

Type	Label (can appear in email notification)	Variable
AS2 Properties	AS2 Payload	%AS2.PAYLOAD%
	AS2 MDN	%AS2.MDN%
	AS2 Local MIC	%AS2.LOCAL_MIC%
	AS2 Remote MIC	%AS2.REMOTE_MIC%
	AS2 Message ID	%AS2.MESSAGE_ID%
	AS2 Host	%AS2.HOST%
	AS2 Transaction Error	%AS2.TRANSACTION_ERROR%
	AS2 Transaction Result	%AS2.TRANSACTION_RESULT%
	AS2 Transaction Verbose	%AS2.TRANSACTION_VERBOSE%
	AS2 Direction	%AS2.DIRECTION%
	AS2 Partner ID	%AS2.PARTNER_ID%
	AS2 EFT Server ID	%AS2.EFT_ID%
	AS2 Content Type	%AS2.CONTENT_TYPE%

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%

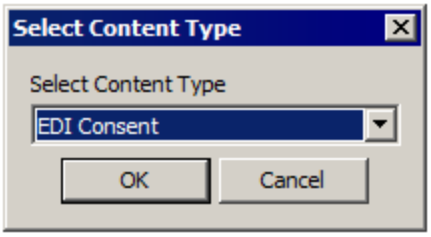
Type	Label (can appear in email notification)	Variable
User Properties	User (Group)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%
Connection Properties	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%

Type	Label (can appear in email notification)	Variable
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%

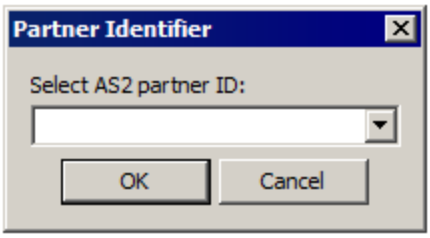
AS2 Conditions

You can apply AS2 Conditions to File Uploaded and AS2-related events.

- **If AS2 Content Type**. Tests whether the AS2 content matches the specified content type.
  1. Add the Condition to a Rule.
  2. In the Rule Builder, click the linked text to specify whether the content type **does/does not** equal to **[specific AS2 content type]**. Click **[specific AS2 content type]** to open the **Select Content Type** dialog box.



  3. Click the **Select Content Type** drop-down list to specify a (**X12**, **EDIFACT**, **XML**, **EDIConsent**, **Binary**, **Plaintext**).
  4. Click **OK**.
- **If AS2 Partner ID**. Tests whether the AS2 Partner ID matches the specified mask.
  1. Add the Condition to a Rule.
  2. In the Rule Builder, click the linked text to specify whether the partner ID **does/does no**t equal to **[specific AS2 Partner ID]**. Click **[specific AS2 Partner ID]** to open the **Partner Identifier** dialog box.



  3. Click the **Select AS2 partner ID** drop-down list to specify a partner.
  4. Click **OK**.

You can also specify the AS2 protocol with the **If Protocol Condition** described in Connection Conditions.

Sending Files to an AS2 Partner via Event Rules

(Requires AS2 module) You can send files via AS2 to a partner for whom you have not previously provisioned an outbound profile by manually specifying that partner's profile in the **AS2 Send File** Event Rule Action. Alternatively, if the AS2 partner has an outbound profile defined, you can select that profile when you define the **AS2 Send File** options.

For example, you could define a Rule with a Timer Event so that every Monday at 8 a.m., all files in a certain folder are sent either to a partner that already has a profile defined on the Server or to a partner that you will define "on the fly" in the **AS2 Send File** dialog box.

The **AS2 Send File to host** Action can be used for Folder Monitor, Timer, and all file-based Events.

UTF-8 filenames/non-ASCII characters are not supported over the AS2 protocol. It is the responsibility of the trading partners to determine the file-naming limits imposed by their trading environments. Refer to RFC 2183, section 2.3 for details of filename parameters.

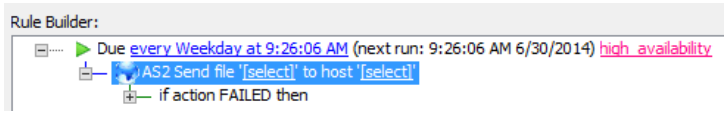
When triggered, the **AS2 Send File to host** Action offloads one or more user-defined files or one or more context files. Depending on the **AS2 Send File to host**Action's retry configuration, the Action fails if any error occurs when attempting to send the AS2 payload. Those errors may include any connection, authentication, transport, or navigation errors; receipting errors or failures; payload errors, including transfer errors or integrity mismatch errors or failures; server communicated errors; and unknown or undefined errors, such as:

- No receipt was provided
- The receipt was not signed
- The MIC value returned did not match the original file/message MIC
- EFT was unable to:
    - verify the receipt signature
    - establish a connection to the remote host
    - upload the file to the remote host
    - send an the receipt asynchronously
    - send the receipt synchronously

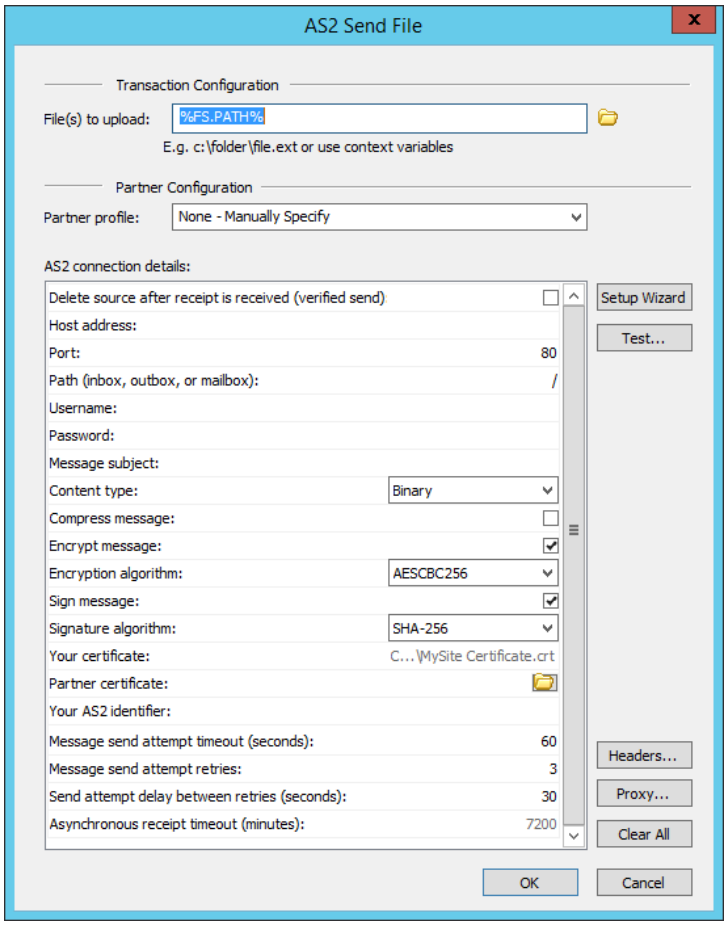
To send files using the AS2 Send File to host Action

1. Create a new Event Rule, such as a Scheduler (Timer) Event. (Refer to Creating Event Rules for details of creating Event Rules, if necessary.)

2. Add the **AS2 Send file to host** Action to the Rule.



3. Click one of the underlined text links. The **AS2 Send File** dialog box appears.



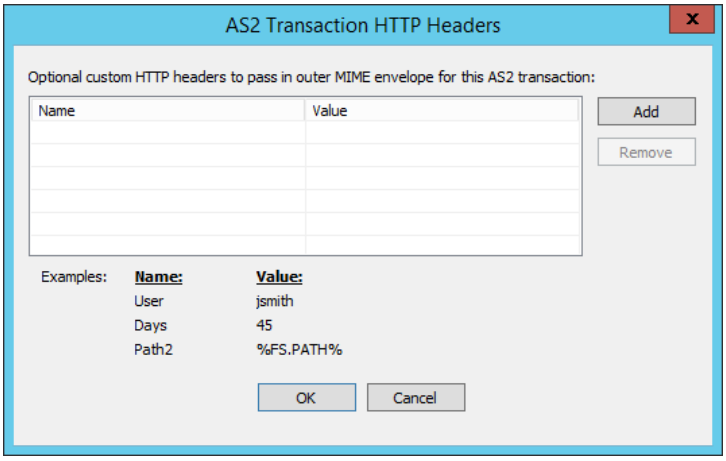
4. In the **File(s) to upload** box, type the path or click the folder icon to specify the file to send to this partner. Include the entire path to the file. You can also use File System context variables such as %FS.PATH% or wildcard masks. For example, to send all files in a folder, type the folder path and ***.***. (The files will not be sent all at once; each file will have a unique message ID.)
5. In the **Partner Configuration** area, specify the AS2 Partner profile using one of the following methods:
    - In the **Partner profile** box, select a defined AS2 outbound partner profile. The fields in the **AS2 connection details** area is completed automatically.

- Provide the connection details in the **AS2 connection details** area. (Refer to AS2 Send File Dialog Box Fields below for details of each field.)
- Click **Setup Wizard** to use the wizard to set up the profile.

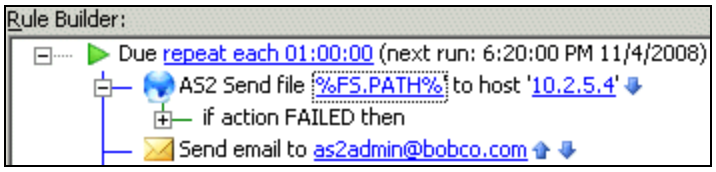
  The **Partner profile** box is linked to the selected profile configuration. If you are using Globalscape authentication, if the profile is updated, the information in the **AS2 Send File** dialog box is updated also; if a referenced profile is deleted, disabled, or not allowed to use AS2, any Event Rule using the profile will fail.

  When you use AD, LDAP, or ODBC authenticated accounts as AS2 partners, if the account in the external database is changed, deleted, or disabled, any Event Rule or Command that references the account will fail. For example, if an AD user SSmith is renamed SJones, you will have to update any Event Rule or Command manually to reflect the new name of the account.

6. To test the configuration, click **Test.**
7. (Optional) Click **Headers**to add a custom header. The purpose of custom HTTP headers is to pass additional or required information to the recipient's server. The **Name** and **Value** fields can each contain up to 255 characters. The **Value** field can use context variables.



   - To add the header, click **Add**, then provide the name and value in the table, as shown in the examples in the dialog box.
8. To configure a proxy server for this partner, click **Proxy**.
9. To clear all of the partner connection details and start over, click **Clear All**.
10. Click **OK** to save the AS2 Partner profile in the Event Rule.
11. Add other Conditions and/or Actions, as needed (for example, add an email notification).



12. Click **Apply** to save the Event Rule on EFT.

AS2 Send File Dialog Box Fields

The AS2 Send File dialog box can be used in Folder Monitor, Timer, and file-based Event Rules. The table below describes each field in the **AS2 Send File** dialog box.

Field	Required/Optional	Description
File(s) to upload	Optional	Used to specify the file(s) to upload to the partner. Can be variables or paths. e.g. **c:\temp\robert.txt** or (if relative path) **\rob.txt** Defaults to %FS.FILE_NAME%; same as if blank. Accepts FS.FILE variables and path strings to drive or UNC paths or relative path where applicable (for example, if using a Folder Monitor Rule).
Partner profile	Required	Used to select a defined partner profile or left blank (the default) if the partner profile is not defined. If blank, complete the fields in the **AS2 Partner profile** area.
Delete source	Required	Used to indicate whether to delete sources files after sending them to the destination, after the MDN is received and verified from the remote AS2 host. Select the check box to delete source files after the MDN is received and verified from the remote AS2 host.
Host address	Required	AS2 outbound host address. **Requires protocol prefix in URL (http:// or https://).** Specified in **AS2 Partner Access** wizard.
Port	Required	AS2 Outbound port. Range is 1-65K
Path (inbox, outbox, or mailbox)	Optional	Relative path (similar to User Home Folder); forward slash (/) by default
Username	Optional	User login name
Password	Optional	Password
Message subject	Optional	AS2 message subject

Field	Required/Optional	Description
Content type	Required	AS2 content type. Options include: • **X12** - Format used by many healthcare, insurance, government, transportation, and finance organizations. • **EDIFACT** - Format adopted by the International Organization for Standardization (ISO) as the ISO standard ISO 9735. • **XML** - File format used for structured documents. • **EDI Consent** - Provides a standard mechanism for "wrapping" the EDI objects but does not specify any details about those objects. • **Binary** (default) - e.g., executables, word processing files, database, spreadsheet, and multimedia files • **Plaintext** - e.g., text and HTML files
Compress message	Required	When selected, specifies that the AS2 message should be compressed when sent. (Cleared by default.)
Encrypt message	Required	When selected, specifies that outbound AS2 messages should be encrypted. (Selected by default.)
Sign message	Required	When selected, specifies that outbound AS2 messages should be signed. (Selected by default.)
Your certificate	Required	Displays the AS2 certificate public key path to use for signing, copied from the Site. (Can be on a drive or UNC path.)
Partner certificate	Required	Specifies the AS2 certificate to use for encrypting outbound transactions and for validating signed MDN receipts. (Can be on a drive or UNC path.)
Your AS2 identifier	Required	Used to apply a unique **AS2-From** ID to outbound messages.
Partner AS2 identifier	Required	Used to apply a unique **AS2-To** ID to outbound messages.
Receipt policy	Required	Used to request an MDN receipt. Options include: • Request a signed receipt (default) • Don’t request a receipt • Request an unsigned receipt
Receipt delivery	Required	Specifies receipt delivery method: Synchronous (default) or Asynchronous Asynchronous receipts will be returned to the domain name specified on the Site's **Connection** tab using the standard or secure listener port specified on that same page (depending on whether you specified HTTP or HTTPS for the remote host value).

The following fields are used to determine whether a message send attempt has failed due to a timeout, error, synchronous MDN receipt failure, or other error, after which EFT will attempt to resend the same message at regular intervals, if specified.

Field	Required/Optional	Description
Message send attempt timeout (seconds)	Optional	Specifies the timeout after which a message send attempt is considered a failure if no response or errors are received from the remote server. Range: 0-600, 60 by default, 0 means no timeout
Message send attempt retries	Optional	Number of times to reattempt to send the message. Range: 0 (no retry) to 999, 10 is the default. Retries do not include the initial attempt. That is, 3 retries means 3 in addition to the first attempt (4 total).
Send attempt delay between retries	Optional	Specifies the time to wait between retries if the send attempt was unsuccessful, in seconds. 30 seconds is the default.
Asynchronous receipt timeout	Optional	Specifies the time to wait for receipt before timing out, in minutes. The default is 7200 minutes (2 hours).

AS2 Variables

Status of AS2 transfers (**available only in AS2-related Event triggers**)

Text Displayed	Variable	Value Contained in Variable
AS2 Content Type	%AS2.CONTENT_TYPE%	Transfer's content type: Application, EDIFACT, XML, Mutually defined EDI, Binary, Plaintext
AS2 Direction	%AS2.DIRECTION%	Direction of the transfer
AS2 EFT ID	%AS2.EFT_ID%	EFT ID used in this transfer
AS2 Host	%AS2.HOST%	Address of the host being sent to (outbound) or received from (inbound)
AS2 Local MIC	%AS2.LOCAL_MIC%	Local AS2 message identification code (MIC)
AS2 MDN	%AS2.MDN%	Message Disposition Notification. The Internet messaging format used to convey a receipt.
AS2 Message ID	%AS2.MESSAGE_ID%	AS2 message identifier
AS2 Partner ID	%AS2.PARTNER_ID%	Transaction partner's AS2 ID
AS2 Payload	%AS2.PAYLOAD%	Name of the file (or an array of file names if MA is used) being transferred over the AS2 session
AS2 Remote MIC	%AS2.REMOTE_MIC%	Remote AS2 message identification code (MIC)
AS2 Transaction Error	%AS2.TRANSACTION_ERROR%	Error (if any) in the AS2 transaction
AS2 Transaction Result	%AS2.TRANSACTION_RESULT%	Overall transaction result (**In Progress**, **Failure**, or **Success**) of the in-context AS2 transaction
AS2 Transaction Verbose	%AS2.TRANSACTION_VERBOSE%	Verbose message for the AS2 transaction

AS2 Transaction Auditing and Monitoring

(Requires AS2, ARM, and HTTP/S module) The topics below provide information about monitoring AS2 transfer activities.

- Introduction to AS2 Transaction Auditing and Monitoring
- AS2 Information in the Database
- AS2 Transaction Reports
- Transfers - AS2 Status Viewer
- Resubmitting AS2 Transmissions
- AS2 Transaction Success and Failure Notifications

Introduction to AS2 Transaction Auditing and Monitoring

The AS2 module provides the following tools to track, monitor, audit, and report on AS2 transactions:

- Transfers - AS2 (status viewer)- A node on EFT's **Status** tab displays a summary of in-progress and recent AS2 transaction history.
- Auditing and Reporting Module (ARM) reports - Predefined AS2 reports provide a summary or details of AS2 transactions. You can also define custom reports.

AS2 Information in the Database

(Requires AS2 and HTTP/S module) The Auditing and Reporting module (ARM) is not required, but is recommended for auditing purposes. (The receipt policy is not dependent on ARM.) EFT provides a sub-node on the **Status** tab that displays a history of AS2 transactions.

The following information is audited to the ARM database:

- Date/Time
- Raw HTTP Headers
- File name
- MDN
- MIC*
- Content Type
- Message-ID
- Remote/Local File path (mailbox)
- Remote/Local Host (hidden by default)
- Status: Success (S), Failure (F), or In Progress (IP)
- Direction: Inbound or Outbound
- EFT AS2 ID
- Partner AS2 ID
- Error (only if Failure) occurred, the verbose error. Otherwise "None".
- Action:
  - Inbound Connection (S, F, IP)
  - Outbound Connection (S, F, IP)
  - Receive File (S, F, IP)
  - Send File (S, F, IP)
  - Send Receipt Asynchronous (S,F,IP)
  - Send Receipt Synchronous (S,F,IP)
  - Receive Receipt (S,F, IP)
  - Receipt Verification (S,F)

*EFT calculates the AS2 MIC using SHA-1. (Refer to RFC 3335 for details.) You can ignore the words "MD5" that appear in the MIC column of the AS2-related reports (**tbl_AS2Transactions** column).

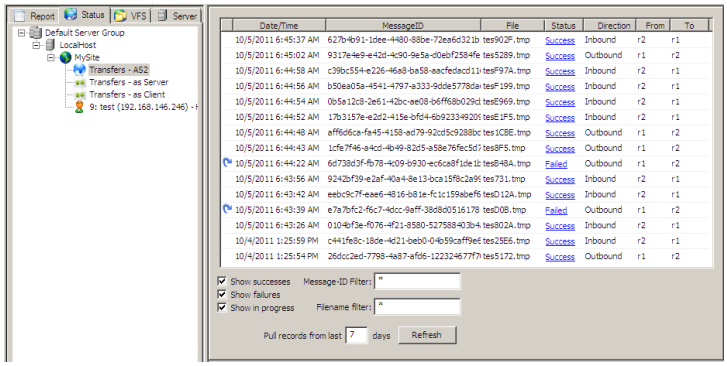
AS2 Transaction Reports

The Auditing and Reporting module (ARM) gathers AS2 data and provides the data in the Transfers - AS2 node and in predefined AS2 reports. You can also define your own custom reports.

- *AS2 Transactions (Summary)* report - A transaction report that displays more detailed information than what is shown on the **Transfers – AS2** node. The report queries all AS2 transactions for the dates specified, grouped by Site, sorted by date, and listed in reverse chronological order. You can add Report Filters for the following data:
  - StartTime
  - MessageID
  - FileName
  - TransactionID
  - FromAS2ID
  - ToAS2ID
  - TransactionStatus (rolled up transaction status)
    - **Success** - File was received/sent MDN successfully received/sent
    - **Failure** - Transaction failed to receive/send after all retries or MDN not received/sent after all retries
    - **In Progress** - Transaction started or is in progress (transferring or waiting for next retry or waiting for MDN, etc.)
- *AS2 Transactions (Detailed)* report - A verbose AS2 file transfer report that provides the information necessary for troubleshooting problem transactions. You can add Report Filters for the following data:
  - StartTime
  - MessageID
  - FileName
  - TransactionID
  - FromAS2ID
  - ToAS2ID
  - TransactionStatus
  - Sitename
  - Error (Displays **None** if there are no errors)

Transfers - AS2 Status Viewer

EFT provides a sub-node on the **Status** tab that displays a history of AS2 transactions.



The **Transfers - AS2** node displays the history of AS2 inbound and outbound transfers, including the result from the MDN. For example, if a file transaction attempt fails 10 times in a row, but succeeds on the 11th attempt and the MDN is sent, the **Transfers - AS2** node reports the transaction as a success. If all of the transaction's file transfer retries fail, then the **Transfers - AS2** node reports the transaction as a failure. If retries are still occurring at the time the **Transfers - AS2** node is invoked, the transaction will be marked as **In Progress**. You can view details of each transaction by clicking its **Status** column. EFT will query and then display (in the default text editor) the details surrounding that transaction as obtained from the ARM database.

When the **Transfers - AS2** node is selected, the last 7 days of transaction summaries are displayed in reverse chronological order. You can change the default of 7 days to display from 1 to 999,999 days of data. Click **Refresh** to display all transactions that may have occurred since the last opening or refresh of the **Transfers - AS2** node.

The node displays the following information:

- **Date and Time** - Last recorded status for the transaction
- **Message ID** - From AS2 header
- **File** - Name of file transferred
- **File Path** - Local inbox or outbox; this column is hidden by default
- **Remote Host Address** - Host address of the sender (Inbound)/receiver (Outbound). This column is hidden by default.
- **Status** - Contains a hyperlink that, when clicked, pulls the *AS2 Detailed* report for that transaction. The report displays transaction details, which is most helpful for in-progress or failed transactions.

  - **Success** - Transaction completed and MDN successfully received/sent
  - **Failure** - Transaction failed to send after all retries or MDN not received/sent
  - **In Progress** - Transaction started or in progress (transferring or waiting for next retry or waiting for MDN, etc.)
- **Direction** - **Inbound** or **Outbound**
- **From** - Server's AS2 ID or the Partner ID (depends on direction)
- **To** - Server's AS2 ID or the Partner ID (depends on direction)

The **Resubmit** icon , to the left of failed transactions, allows you to resubmit the file (s) and/or MDN(s). You can also resubmit a file, or group of files by multi-selecting failed transaction rows, then right-clicking and clicking **Resubmit**. If you resubmit a file that is a part of multi-file transaction, all of the files will be resubmitted. You can only resubmit failed transactions. You cannot resubmit in-progress or successful transactions.

Customizing the Display

You can customize the **Transfers - AS2** status viewer to suit your needs:

- Choose the columns to display or hide by right-clicking on a column header, then selecting/clearing the column name in the submenu.
- Sort by a specific column in ascending or descending order by clicking the column header.
- Define filters to display or hide rows based on **Status**, **Message-ID**, or **File Name**.
  - To filter the display based on status, select or clear the **Show successes**, **Show failures**, and **Show in progress** check boxes, and then click **Refresh**
  - To filter the display based on the message-ID, in the **Message-ID** box, type the message ID, and then click **Refresh**.
  - To filter the display based on the filename, type a name in the **Filename** box, and then click **Refresh**.
  - To change the number of days of history to display, in the **Pull records from last**<*n*>**days** box, type the number of days, from 1 to 9999.
- Refresh or clear the display by right-clicking an empty row, and then clicking **Refresh**, or in the filter area, click **Refresh**.

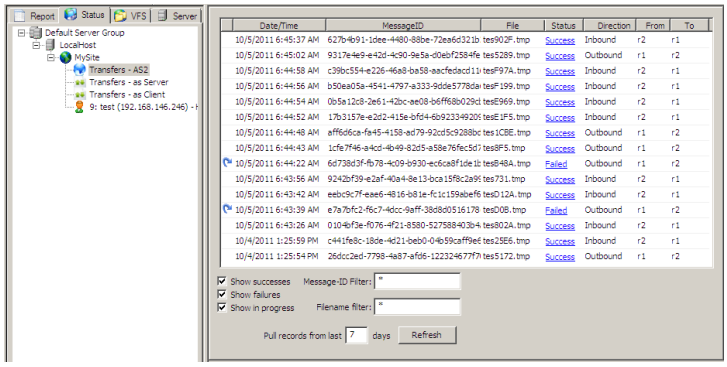
Resubmitting AS2 Transmissions

In the **Transfers - AS2** node, the **Resubmit** icon to the left of failed transactions allows you to resubmit the file(s) and/or MDN(s). You can only resubmit failed transmissions. You cannot resubmit in-progress or successful transmissions.

- **Outbound**. If a failure was an outbound transaction (failed after all retries and the MDN was never received), you can attempt to send the same file again.
- **Inbound**. When an inbound transaction fails, resubmit is allowed only when the failure was due to a failure in sending the receipt (MDN). (EFT cannot resubmit the file, because it did not send it to begin with.) The resubmit action attempts to resend the MDN receipt.

To resubmit a transmission

1. In the administration interface, connect to EFT, and click the **Status** tab.
2. Expand the Server and Site nodes, and then click the **AS2 Transactions** node. The Site's AS2 transactions appear in the right pane.



3. Click in the row of the failed transaction to select it, and then click the **Resubmit** icon . A confirmation prompt appears.
4. Click **Yes**. The transaction is resubmitted and appears in a new row. The resubmitted transaction populates a new row in the **Transfers – AS2** node with the new transaction and new message ID.

   There can be multiple rows (other transmissions) between the failed transmission and the resubmitted transmission.

AS2 Transaction Success and Failure Notification

EFT can execute a command or send an email to notify you of the success or failure of AS2 transactions. The email or Command is triggered when all message send attempts have been attempted or the asynchronous MDN wait time has expired (if applicable).

The email notification and custom command are configured by clicking the applicable link in the **AS2 Inbound** and **AS2 Outbound** tabs or in the AS2 Partner Access wizard.

- Clicking the Transaction FAILED/SUCCESS notification email link, **[Add]**, opens the Edit Mail Template dialog box.
- Clicking the Transaction FAILED/SUCCESS send command link, **[Add]**, opens the Custom Command dialog box. (You will have to define the custom command before using it in the notification.)
- Each of the fields are optional

Field	Description
Transaction FAILED notification email	Opens the **Edit Mail** dialog box in which you can specify an email notification for failed transaction.
Transaction SUCCESS notification email	Opens the **Edit Mail** dialog box in which you can specify an email notification for successful transaction.
Transaction FAILED run command	Opens the **Custom Command** dialog box in which you can specify a **Command**to run upon failed transaction.
Transaction SUCCESS run command	Opens the **Custom Command** dialog box in which you can specify a **Command**to run upon successful transaction.

- Refer to email Notification Action for details of defining an email notification.
- Refer to Creating a Command to create a command and refer to Script: Custom Command Action for details of using a Command.

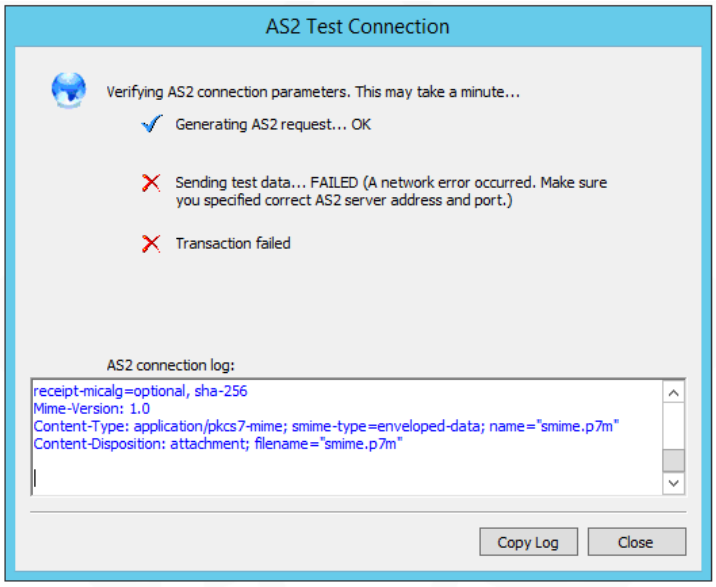
Related Topics

- Creating a Command
- The Custom Command Wizard
- email Notification Action
- Creating an email Notification Template

Testing the AS2 Outbound Connection

(Requires AS2 and HTTP/S module) You can validate the AS2 partner configuration details by sending a test file to the remote partner. This provides immediate feedback as to whether an outbound connection was configured properly.

On the **AS2 Outbound** tab or in the **AS2 Send File to host** Event Rule Action, click **Test** to send a test file to the AS2 host specified. The **AS2 Test Connection** dialog box appears.



EFT attempts to send a test file using the parameters supplied and displays a success or failure message along with the entire log. The test determines success of the following parameters:

- Presence of certificates necessary to sign and/or verify signatures
- Connection to the host and navigation to the correct path
- Upload of the test file
- Receipt and verification of the MDN receipt
- Transaction completed

A blue check indicates success; a red X indicates failure. The HTTP request and response headers are displayed in the **AS2 connection log** below the success/failure list. You can copy the log to a text file or email for troubleshooting.

If you click **Close** before the test is complete, the test ends and no results are displayed or saved.

To copy the log for troubleshooting/emailing

1. After the test complete, click **Copy Log**. The log is copied to Windows Clipboard.
2. In the document or email, click **Paste**.

In the Auditing and Reporting database, the filenames are clearly test files (for example, **tes1.tmp**) to indicate that an audited transaction is a test. However, test transactions are treated the same as any other AS2 transaction and appear in the database the same as any other AS2 transaction.

Related Topics

- Configuring Outbound AS2 Parameters
- Sending Files to an AS2 Partner via Event Rules
- Troubleshooting AS2 Connections

Troubleshooting AS2 Issues

(Requires AS2 and HTTP/S module) The AS2 module provides monitoring tools that can assist you in troubleshooting AS2 connections to EFT. See also: Testing the AS2 Outbound Connection.

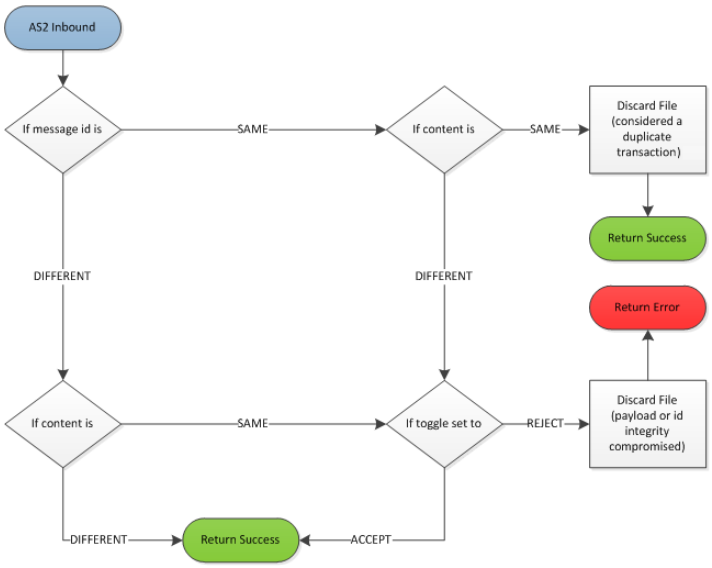
Possible reasons for AS2 file transfer failure:

- An inbound unencrypted transmission over HTTP
- An upload attempt to a folder where user doesn't have write access
- If sender's EFT is configured to redirect all HTTP to HTTPS and receiver doesn't allow this while receiving the data
- SSL certificates/keys mismatch
- Incorrect IP adddress/port/folder path

Below are some important things to consider when troubleshooting failed AS2 connections:

- **Ensure that your partner-provided information (AS2 ID, certificates, host information) is accurate** and that your provider has configured your account correctly on the remote server.
- **Provide your certificate file (public key) to your partner and obtain your partner's public key** (unless your partner will be sending you non-encrypted, non-signed messages that do not request an MDN).
- **Send a test file to your partner**. The **Test**button on the **AS2 Configuration** wizard sends a test file to a defined AS2 partner to verify connection. The success or failure results are displayed in a prompt that contains each stage of the transfer. The stages include the presence of certificates necessary to sign and/or verify signatures, connection to the host and navigation to the correct path, upload of the test file, and receipt and verification of the MDN receipt. The complete HTTP sent and received headers are captured and displayed in a list box under the success/failure stages. You can select and copy the text of this log for analysis. The maximum allowed file size for AS2 transfers is 20GB.
- **Contact your partner and ask them to connect and transfer a test file to EFT.** If the test is not successful, examine reports and the **Transfers - AS2** node in EFT:
    - ARM report - *AS2 Transactions (Detailed)*- Review the report to determine why the problem transaction occurred.
    - Transfers - AS2 node - Review the sub-node on the **Status** tab to view recent AS2 transactions (retrieved from EFT's ARM database) to identify possible configuration errors.

- **AS2 partner receives multiple MDN failures when sending to EFT in HTTPS.** Turn off the "100 Continue" reply by selecting the **HTTP 1.0 mode** check box in the **AS2 Inbound Settings** dialog box for the partner's account. Refer to AS2 Inbound Parametersfor more information about "100 Continue."
- EFT does not support UTF-8 filenames over AS2.
- **EFT is sending multiple success messages.** If the ID and payload are the same as a prior incoming message, EFT will reject the payload but will send a "success" message back to the client. So if a client resends a package for some reason, EFT will resend the success message. Below is a diagram that demonstrates how EFT manages incoming messages.



AS2 and the Auditing and Reporting Module

You must have the Auditing and Reporting module installed to use the AS2 module. If the ARM database is not installed, configured properly, or fails, AS2 functionality is not available.

If ARM is not installed, configured, or connected:

- For outbound AS2 transactions, the transaction is cancelled, and EFT sends emails, execute commands, and triggers events. (This includes any outbound transaction, whether initiated by AS2 Send File Action or by folder monitor specified in partner AS2 outbound tab.)
- For inbound transaction, EFT replies to the partner with "500 Internal server error: database failure," then sends emails, executes commands, and triggers events.

AS2 Error Warnings and Prompts

(Requires AS2 and HTTP/S module) EFT provides error warnings and prompts when you are configuring the AS2 module and when you are sending/receiving files using AS2.

AS2 Configuration Errors

EFT presents a prompt and disallows changes to AS2 configuration in the following instances:

- Settings are enabled that require a partner AS2 certificate and no certificate has been defined for that partner
- Settings are enabled that require EFT's AS2 certificate and no certificate has been defined for EFT
- Settings are enabled that require the partner's or the Server's identifier and no identifier has been defined for the partner or EFT
- The chosen certificate is set to expire in 30 days or fewer
- A certificate being imported is a combined certificate
- You open the **AS2 Send File** dialog box and click **OK** or **Apply** without specifying a partner profile.

AS2 Transfer Errors

EFT provides the following transfer error messages. When you receive one of these errors, you should examine your AS2 configuration and other Site/User settings. Certain messages are simply an indication that the configuration is working as designed. For example, if your AS2 outbound configuration has a filter mask to ban files with a .**zip** extension or if the Site's configuration bans files of this type on the Server, you will receive a banned file message when a user attempts to send files of this type.

Error	Possible Cause/Solution
A network error occurred	Verify AS2 server address and port; ensure there is a connection between the two servers and nothing is blocking the connection; require SSL certificates from connected clients might be enabled; SSL negotiation failed; retry transfer
Error decoding certificate	AS2 module cannot decode EFT's or partner's certificate. Make sure the certificate is not corrupt or is of an unsupported format. Also check that the certificate is a single certificate and not multiple certificates inside of a certificate.

The receipt was unsigned and a signed receipt was expected	Incorrect certificate used for EFT or partner certificate
Incorrect AS2-From field	Incorrect "Your AS2 identifier"
Incorrect AS2-To field	Incorrect "Partner AS2 identifier"
RSA Error: Inadequate amount of padding in encrypted message	AS2 module cannot verify signature of signed incoming message; possible problem with identifiers; sender might be using incorrect identifier; AS2 MDN cannot be verified
Timeout occurred while sending MDN	Firewall blocking receipt send (MDN blocked)
File already exists, Message with duplicate ID and different payload was received.	(Tried to overwrite existing file and corresponding policy is set to **Reject**.) AS2 configuration does not allow overwriting files of same name; change AS2 configuration to Accept these files or move/rename files after they are received.
Quota exceeded	File is too large. User configuration does not accept files of this size; ***Specifying User Disk Quota* on page 1036** or compress/split file.
File is banned	(Uploaded file meets Site's "Ban" mask) Site configuration does not accept files of this type/name. ***Banning Unwanted File Types* on page 838** or let your partner know that files of that type cannot be uploaded to EFT.
Use encryption or HTTPS	(Tried to use "plain" AS2 without encryption.) AS2 configuration must be set to use encrypted HTTP or HTTPS. Or use redirection; refer to ***Redirecting HTTP to HTTPS* on page 685** for details of redirection.
Unable to decrypt message, RSA Error	Inadequate amount of padding in encrypted message. AS2 module cannot decrypt encrypted incoming message.
HTTP error: 400 Bad Request	Receiver/sender has incorrect or missing certificate; Connection problem of some kind
HTTP error: 401 Unauthorized	Authentication failed for username/password; IP address is blocked
HTTP error: 403 Forbidden	Incorrect folder location, Mailbox path; do not have permission to remote folder/path; AS2 is not enabled/supported on receiving side

Connection Settings

Protocols are enabled/configured on the Site and inherited by the Settings Templates and user accounts. (You can then configure the Settings Templates and user accounts differently, if needed.) Before configuring SSL on the Site, you must configure SSL and FIPS-approved connections on the Server's **Security** tab. The topics below provide the procedures for configuring connections and protocols on Sites, Settings Templates, and user accounts.

- Connection Limits Dialog Box
- User Limit Reached Message
- Quit Session Messages
- Protocol Settings

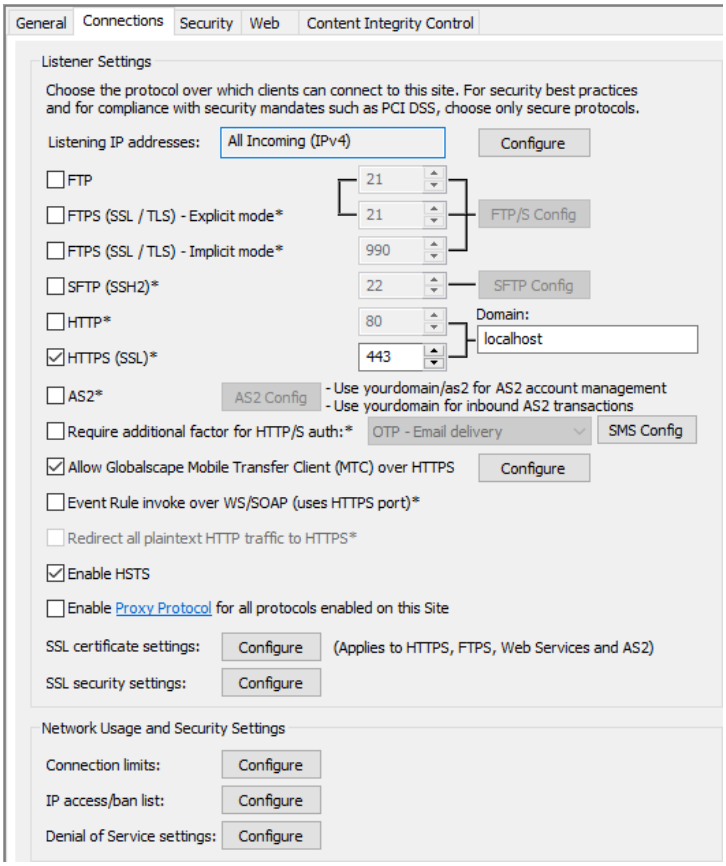
Protocol Settings

EFT supports the following protocols: FTP/s, HTTP/s, AS2, SFTP, and SSL. The protocols are configured on an EFT Site and then can be enabled or disabled on the Site or Settings Template, or for each user. (SSL must first be enabled/configured on the Server.) The client, not the server, drives the authentication process. That is, if you specify a protocol that the client doesn't use, the client will not be able to connect.

If the check box contains a gray check mark, the user or Settings Template is inheriting permission from its parent.

To enable a connection protocol

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site, Settings Template, or user account that you want to configure.
3. In the right pane, click the **Connections**tab.



4. Do one or more of the following:

- To allow/disable FTP access, select/clear the **FTP** check box, and then click **FTP Config**to configure FTP Settings.
- To allow/disable FTPS (SSL/TLS) access, select/clear the **FTPS (SSL/TLS)** check box, then click **FTP Config** to configure FTP Settings, and next to **SSL certificate settings**, click **Configure**to configure SSL certificate settings.
- To allow/disable the SFTP access, select/clear the **SFTP (SSH2)** check box, and then click **SFTP Config** to configure SFTP authentication options.
- To allow/disable HTTP access, select/clear the **HTTP** check box.
- To allow/disable HTTPS access, select/clear the **HTTPS (SSL)** check box, then, next to SSL Certificate settings, click **Configure** to configure SSL certificate settings.
- To allow/disable AS2access, select/clear the **AS2**check box. (This check box is disabled if HTTP or HTTPS is disabled.) Click **AS2 Config** to configure AS2 connections to the Site, then, next to **SSL certificate settings**, click **Configure** to configure SSL certificate settings.
- To allow/disable Web Services, select/clear the **Enable Web Services** check box.
- To redirect all plaintext HTTP traffic to HTTPS, select the **Redirect all plaintext HTTP traffic to HTTPS (enable HSTS)** check box. (**HTTPS**must be selected first.)
- To enable account management over HTTP or HTTPS, select the **Enable account management over HTTPS** check box. The IP address for account management appears in the adjacent text box. It is not editable, but you can copy it to paste into emails.
- To enable WTC access (on the Settings Template or user account), select the **HTTPS** check box, then select the **Allow Web Transfer Client (WTC) over HTTP/S** check box.

5. In the **Domain**box, specify the fully qualified domain name that is to be used for HTTP, HTTPS, and AS2 connections, account management, email template links, Workspaces invitations, and so on. For scClient to provide accelerated transfers, the address in the **Domain**box must be the DMZ Gateway IP address.
6. Click **Apply** to save the changes on EFT.

Related Topics

- Listener (Protocol) Settings
- Enabling SSL on the Server

- FIPS (Federal Information Processing Standard) (enabled on the Server's **Security** tab)

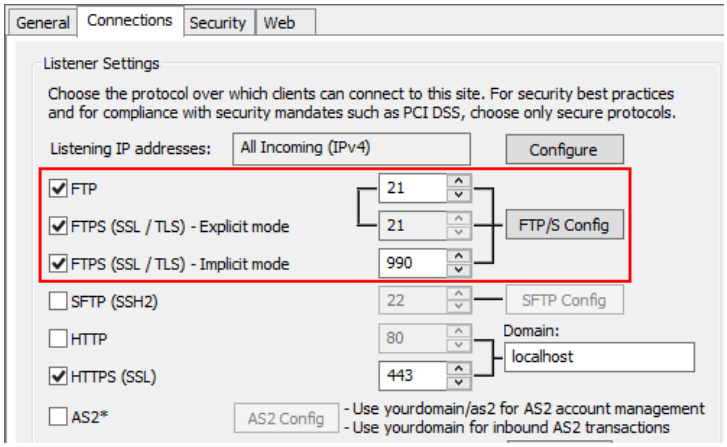
Connection Banner Message

When a client first connects to the Site via FTP, but before the user logs on, the *connection banner*appears. For example:

```
[8/25/2009 9:47:43 AM] 220 Globalscape EFT * UNREGISTERED COPY
*
```

(`UNREGISTERED COPY`appears until you activate your serial number.)

- The FTP connection banner message is configured in the **FTP Settings** dialog box on the Site.

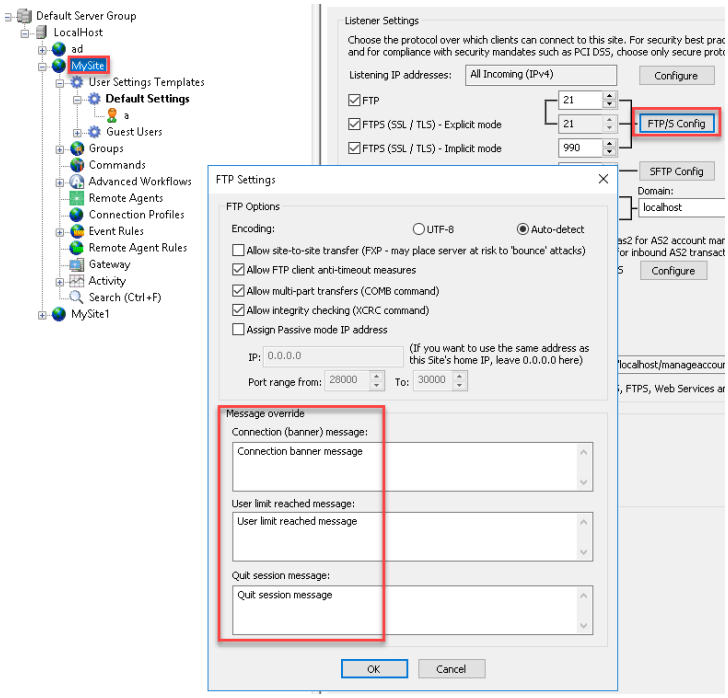


- EFT sends two banners in **FTP or FTP/s** connections:
  1. EFT displays a ***connection banner*** immediately after a client connects via FTP (before requesting the login credentials).
     - The **connection**banner can be edited at the Site level in **FTP/S Config**.
  2. EFT displays a ***login banner*** after the client provides the login credentials and the credentials are authenticated.
     - The **login** banner can be edited at the Settings Template (or user account) level in **FTP Config**.
- EFT only sends one banner (Site level) for **SFTP**connections. When the SFTP banner is sent to the client, EFT does not populate variables due to restrictions with the protocol.
  - The message defined in the Settings Template **FTP Settings** dialog box is sent to the client **after**the user logs in.

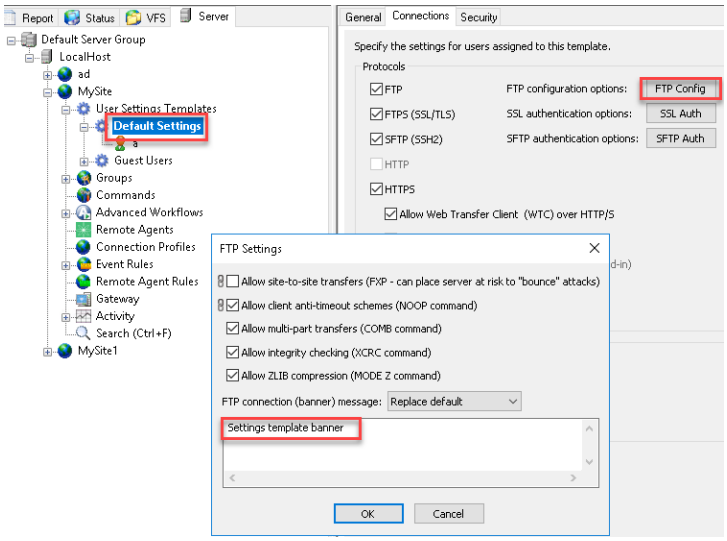
- In the Settings Template or user account, you can specify the following alternatives: use default message ("Login OK, proceed."), add to default, replace default, or None (show no banner at all).
- SFTP connections use the default connection banner in the **FTP Settings** dialog box on the Site or a ***login***message on the Settings Template (or user account) instead of the default connection banner.

- **FTPS** only allows DATE and TIME variables in the initial **connection**message on the Site.
  - FTPS allows other variables to be listed in the Settings Template (or user account) banner: %USER.Full_Name%, %USER.LOGIN%, %USER.EMAIL%, %USER.FIRST_NAME%, and %USER.LAST_NAME%

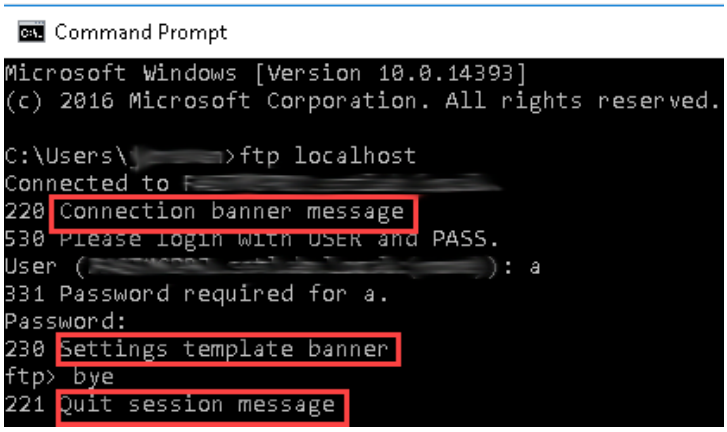
Configuring the FTP banner:



Configuring the Settings Template or SFTP banner:



FTP login sequence:



To modify the connection banners, refer to Configuring FTP or FTPS.

User Limit Reached Message

You can configure a Site to allow only a specified number of maximum simultaneous connections. If you click this option, you can specify a message for users when the maximum simultaneous connections is exceeded.

You can display a message unique to Settings Template or user in addition to or instead of the Site's message. Users automatically inherit the default message applied to their Settings Template.

The **User limit reached message**also can be used to define the login message for SFTP connections. Refer to Connection Banner Message.

To modify the maximum connections message

1. Open the **FTP Settings** dialog box.
2. In the **User limit reached message** box, specify the message you want to display
3. Click **OK** to close the dialog box.
4. Click **Apply** to save the changes on EFT.

Quit Session Message

EFT can send an exit message when the client closes the session gracefully by using the FTP QUIT command. You can display a message unique to a user in addition to or instead of the Site's FTP banner message. Users automatically inherit the default message applied to their Settings Template.

To modify the Quit Session message

1. Open the **FTP Settings** dialog box.
2. In the **Quit session message** box, specify the exit message to display.
3. Click **OK** to close the dialog box.
4. Click **Apply** to save the changes on EFT.

Content Integrity Control

The following topics describe the Content Integrity Control (CIC) configuration. (See also File: Scan Action under Event Rules.)

- Content Integrity Control Tab
- Create a CIC Profile
- ICAP Options

Create a CIC Profile

The Content Integrity Control (CIC) profile is used in the **File: Scan** Action to allow ICAP clients to pass HTTP messages to ICAP servers to scan the file(s) in the Event Rule that is passing through EFT.

You can create reusable profiles on the Content Integrity Control Tab as you need it.

To create a profile to be used in the File Scan Action (CIC)

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the node of the Site you want to configure.
3. In the right pane, click the **Content Integrity Control** tab.
4. Click **Add**. The tab becomes editable.
5. **Profile name**- Provide a descriptive name for the profile
6. **Host**, **Path, Port** - These settings depend on settings in the antivirus or DLP (ICAP) server.
    - The **Host**field cannot be blank.
    - By default, the port is set to 1344.
7. **Mode** - Specify one of the following:
    - **Request modification (REQMOD)** Request modification mode - Embeds file contents in an HTTP PUT request body, which is then sent in the body of an ICAP request to the server. The ICAP server may respond with a modified version of the embedded request, or a new HTTP response. The ICAP response will depend on your ICAP server's implementation.
    - **Response modification (RESPMOD)** Response modification mode - Embeds file contents in an HTTP 200 OK response body, which is then sent in the body of an ICAP request to the server. The ICAP server may respond with a modified version of the embedded response. The ICAP response will depend on your ICAP server's implementation.
8. **Test Connection**- After you specify the connection to the ICAP server, test the connection. If connection fails, verify these settings match the settings defined in the antivirus or DLP solution.
9. **Limit scans to first**- (Optional) Specify the number of bytes to scan. Some antivirus solutions only require a subset of a file's contents to test against their database of malware signatures. To keep from transferring large files in their entirety when we only need the first X bytes, you can specify how many bytes are sent to the ICAP server.

When this check box is cleared, the entire file is transferred to the ICAP server. If the file is smaller than the size you've specified, the entire file will be transferred for processing.

10. (Optional) **Headers** - Only set these values if needed for problematic ICAP connections. These headers are used in the ICAP server logs.
    - **HTTP host** - The EFT site's local host address (do not use "localhost")
    - **X-Client-IP, X-Server-IP, X-Subscriber-ID, X-Authenticated Groups** - Blank by default
    - **X-Authentication User** - Provide a string with variables.
        - **LDAP** - Example: "LDAP://pdc/samaccountName=%LOGIN.LOGIN%,DC=s5development,DC=local"
        - **AD** - Examples: WinNT://{NetBIOSDomainName/sAMAccountName}, WinNT://pdc/s5dev\arybin
        - **Other** - Examples: Local://%USER.LOGIN%, Local://%SERVER.NODE_NAME%
        - User can override and use context variables if desired as field elements. EFT will base-64 encode.
11. Under Response handling, specify whether to content should be blocked when the following occur: **Connection errors**, **HTTP errors**, or **ICAP redactions**.
12. (Optional) **Audit and put into variables these ICAP response "X-" headers** - Specify “X-“ headers for auditing using ARM. If this option is enabled and no “X-“ headers are specified, all “X-“ headers will be audited. Use semicolons between multiple items. Note this check box only affects whether the specified headers are audited by ARM, regardless of success or failure.
13. Click **Apply**to save the new profile. The new profile name appears in the **Profiles** list and is now available in the **Content Integrity Control**dialog box in the File Scan Action.

ICAP Options

ICAP Options

EFT v8.0.5 and later support the use of ICAP Options method. The ICAP "OPTIONS" method is used by the ICAP client to retrieve configuration information from the ICAP server. In this method, the ICAP client sends a request addressed to a specific ICAP resource and receives back a response with options that are specific to the service named by the URI. All OPTIONS requests MAY also return options that apply to all services.

Wireshark capture of OPTIONS RESPMOD from Clearswift:

OPTIONS icap://192.168.100.79:1344/policy_service_resp ICAP/1.0

Host: 192.168.100.79

ICAP/1.0 200 OK

Server: Traffic Spicer 2.4.0

ISTag: "CSICAP/v2.4.0/cd7ac05/CSAdapter"

Methods: RESPMOD

Preview: 0

Allow: 204

Max-Connections: 980

Transfer-Preview: *

Encapsulated: null-body=0

X-Include: X-Client-IP, X-Server-IP, X-Authenticated-User, X-Authenticated-Groups

Wireshark capture of OPTIONS REQMOD from Kaspersky:

OPTIONS icap://192.168.100.81:1344/av/reqmod ICAP/1.0

Host: 192.168.100.81

ICAP/1.0 200 OK

ISTag: "KAVPROXY"

Date: Fri, 05 Feb 2021 20:53:22 GMT

Methods: REQMOD

Allow: 204

Service: KAV-ICAP-Sever/5.5

Preview: 0

Max-Connections: 5000

Service-ID: KAVIcap

X-Include: X-Client-IP

Transfer-Preview: *

Transfer-Ignore:

Options-TTL: 300

Encapsulated: null-body=0

Wireshark capture of OPTIONS RESPMOD from Symantec:

OPTIONS icap://192.168.100.82:1344/RESPMOD ICAP/1.0

Host: 192.168.100.82

ICAP/1.0 200 OK

ISTag: "Vontu14.5"

Methods: RESPMOD

Options-TTL: 3600

Preview: 0

Transfer-Preview: *

Allow: 204

X-Include: X-Client-IP, X-Authenticated-User

Encapsulated: null-body=0

Max-Connections: 16

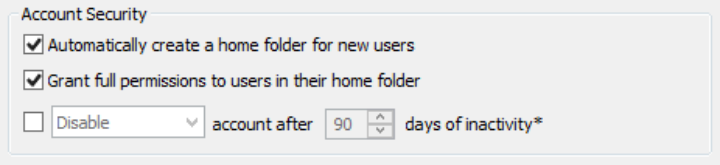
Automatically Creating a Home Folder for New Users (Site)

EFT can automatically create a home folder for new users, and grant full permissions to those users in their home folders. You can set this on the Site, Settings Template, and/or for each user. Each child inherits from its parent, but you can override that setting.

This setting only applies to automatically created user accounts, not the accounts manually created by an administrator.

To automatically create home folders for automatically created new users on the Site

1. In the administration interface, ***Logging In to Administer EFT* on page 281** and click the **Server**tab.
2. On the **Server**tab, click the Site that you want to configure, and then click the **Security** tab.
3. In the **Account Security**area, select the **Automatically create a home folder for newly added users** check box.



4. To allow the users full permissions in their folders, select the **Grant full permissions to users in their home folder** check box.
5. Click **Apply**to save the changes on the Server.

Related Topic

- Automatically Creating a Home Folder for New Users (Site)
- Specifying a User's Home Folder
- Setting the Home Folder for AD-Authenticated Users

Azure Data Lake Storage

Azure Data Lake Storage is a highly scalable and cost-effective data lake solution for big data analytics. Data Lake Storage Gen2 extends Azure Blob Storage capabilities and is optimized for analytics workloads. EFT Event Rules allow you to store files in or monitor for added files in Azure's Data Lake generation 2 (ADLSg2), so that you can reduce cost when compared with saving files into a standard blob storage.

Containers created with ADLSg2 support can be monitored by a Folder Monitor Event as long as the Azure container credentials and Active Directory domain trust relationship is enabled.

To use a Folder Monitor Event to monitor an Azure file share, be sure to enable the VFS overrideand create a virtual folder that points to the Azure file share path.

EFT Secrets Primer (Knowledgebase)

From https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-introduction:

The following are the equivalent entities, as described by different concepts. Unless specified otherwise these entities are directly *synonymous*:

Concept	Top Level Organization	Lower Level Organization	Data Container
Blobs – General purpose object storage	Container	Virtual directory (SDK only – does not provide atomic manipulation)	Blob
Azure Data Lake Storage Gen2 – Analytics Storage	Container	Directory	File

Related Topics

- Configuring Azure Key Vault Support for EFT
- Configuring the Secrets Module
- Override VFS Credentials
- Folder Monitor Event

Banning Unwanted File Types

EFT can block the upload or download of certain files. You can specify which files to block using wildcards (? for 0 or any 1 character or * for 0 or more characters) or exact file names.

For example, to block a file called **virus.wav**, you can type any of the following:

`virus.wav`

(blocks the specific file)

`*.wav`

(blocks all wav files)

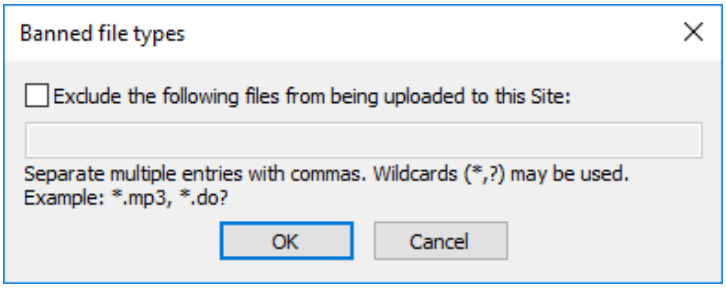
`*.wa?`

(blocks all files with 2 or 3 character extensions that start with wa. Note that ".do?x" only bans .docx files.)

Take extra care when using wildcards to block files so that you do not block files that you want to allow.

To ban files

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Security** tab.
4. In the **Data Security** area, next to **Banned file types**, click **Configure**. The **Banned File Types** dialog box appears.



5. Select the **Exclude the following files from the Site** check box, then type the filename or wildcard representation (*.mp3 or *.mp?) for the file(s) you want to exclude from the Site. Separate multiple entries with commas.

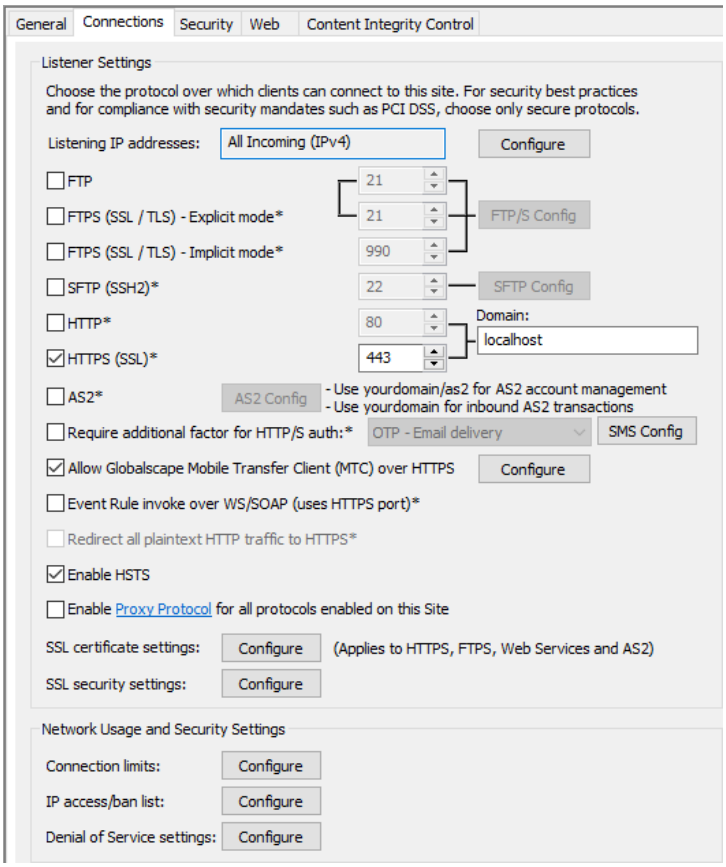
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

Changing a Site's IP Address or Port

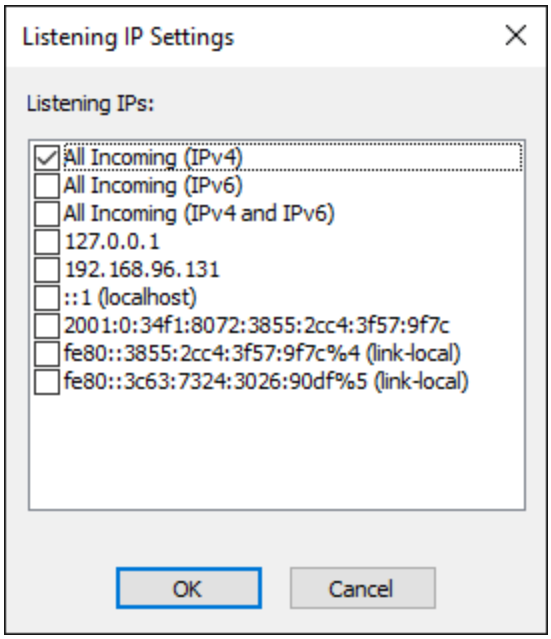
A Site's IP address and port are specified when the Site is created. You can change the IP address and ports using the procedure below.

To change the listening (incoming) IP address and/or port

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Connections** tab.



4. Next to the **Listening IP addresses** box, click **Configure**. The **Listening IP Settings**dialog box appears.



- The dialog box displays the IP addresses that are available on the computer, in addition to **All Incoming (IPv4)**and **All Incoming (IPv6)**.
- You cannot type in an address.
- IPv6not enabled by default for security reasons; IPv4 enabled by default.
- The "All" options are exclusive. That is, you can't select **All Incoming (IPv4)** and then one or more specific IP addresses. However, you can select multiple individual addresses if none of the All options are selected.
- "Link local" appears next to certain IPv6 addresses. Routers do not forward packets with link-local addresses. In IPv6, link-local addresses are always assigned, automatically or by configuration, and are required for the internal functioning of various protocol components. IPv6 requires operating systems to assign link-local addresses to network interfaces even when routable addresses are also assigned. A link-local unicast address has the prefix fe80::/10 in standard IPv6 CIDR notation.

5. Select one or more check boxes for the IP addresses on which the Site is to listen for connections, and then click **OK**. The selected addresses appear in the **Listening IP addresses**box.
    - You can copy the addresses in the **Listening IP addresses**box: Right-click in the box, click **Select All**, then right-click again and click **Copy**or use CTRL+V. (Unicode-related items on the right-click menu are a Windows feature and do not apply to EFT.)
6. Specify the port number for each of the enabled protocols.
7. Click **Apply** to save the changes.

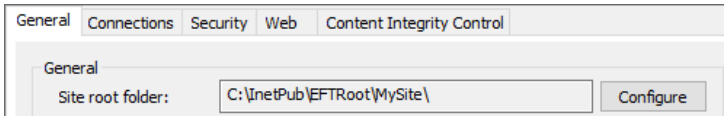
8. A confirmation prompt appears. Click **Yes**to apply the changes and restart the Site or click **No**if you do not want to restart the Site. (Changes will be applied at the next restart.) **Cancel**returns you to the tab where you can click **Refresh**to remove your changes.

Changing a Site's Root Folder

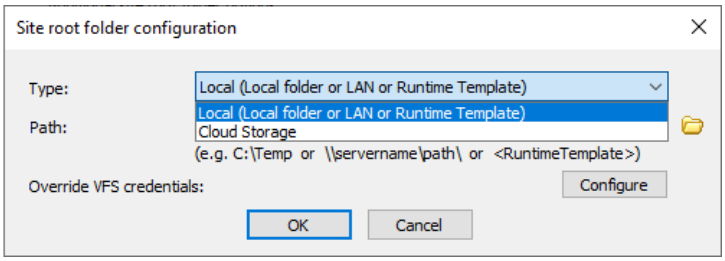
The Site root folder is specified when you create a new Site; however, you can later change a Site's root folder.

To change the Site root folder

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **General**tab.

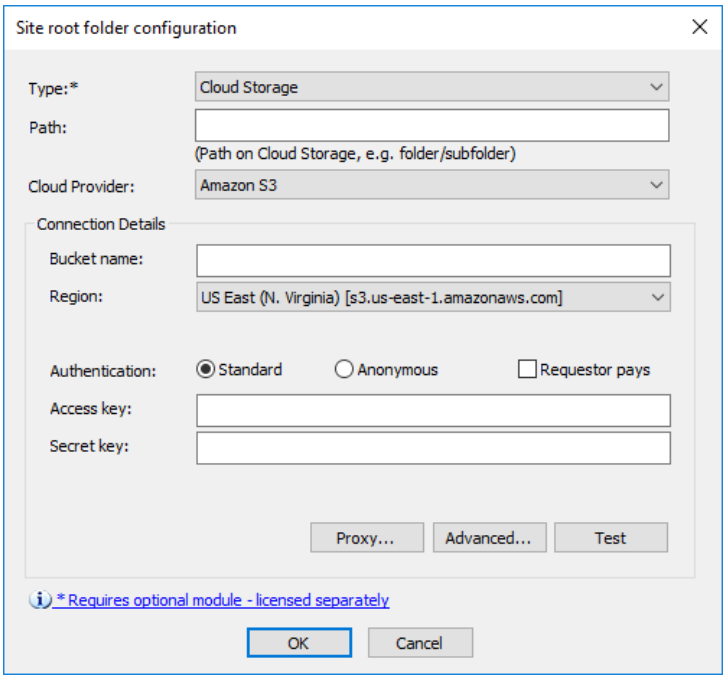


4. Next to the **Site root folder** box, click **Configure**. The **Site root folder configuration** dialog box appears.



5. Specify a new Site root folder. Use the drop-down list to specify **Local folder, LAN, Runtime Template** or **Cloud Storage**, the specify the new path.
    - If you selected **Cloud Storage**, the dialog box expands to display cloud configuration.

    > **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.



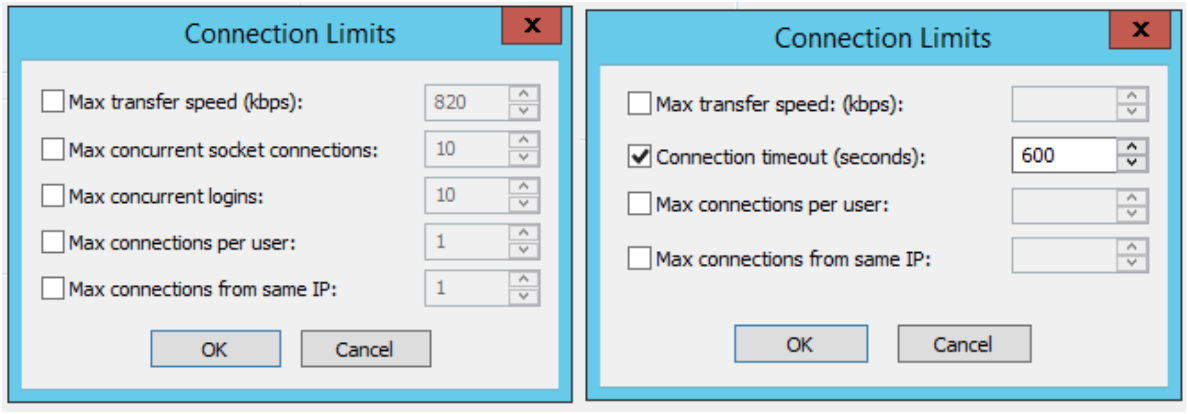
- Under **Cloud Provider**, provide the connections details and authentication for cloud storage. Refer to Defining a Connection Profile for details of how to define the details.

6. Click **Apply**to save the changes on EFT.

Because of a limitation of the HTTP protocol, when a connection is established using HTTP, the client (for example, a Web browser) shows the root folder, not the user's home folder.

Connection Limits Dialog Box

The **Connection Limits** dialog box is used to set maximum speed, logins, and connections, on a Site, Settings Template, or user account.



To open the Connection Limits dialog box

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site, Settings Template, or user account that you want to configure.
3. In the right pane, click the **Connections**tab.
4. In the **Network Usage and Security Settings** area, next to **Connection limits**, click **Configure**. The **Connection Limits** dialog box appears.

   Refer to the following procedures for details of these settings:

   - Setting Maximum Transfer Speeds
   - Setting Maximum Concurrent Socket Connections (Site only)
   - Setting Maximum Concurrent Logins (Site only)
   - Setting Maximum Connections per User
   - Setting Maximum Connections per IP Address
   - Disconnecting Users on Timeout
5. Click **OK** to close the dialog box.
6. Click **Apply**to save the changes on EFT.

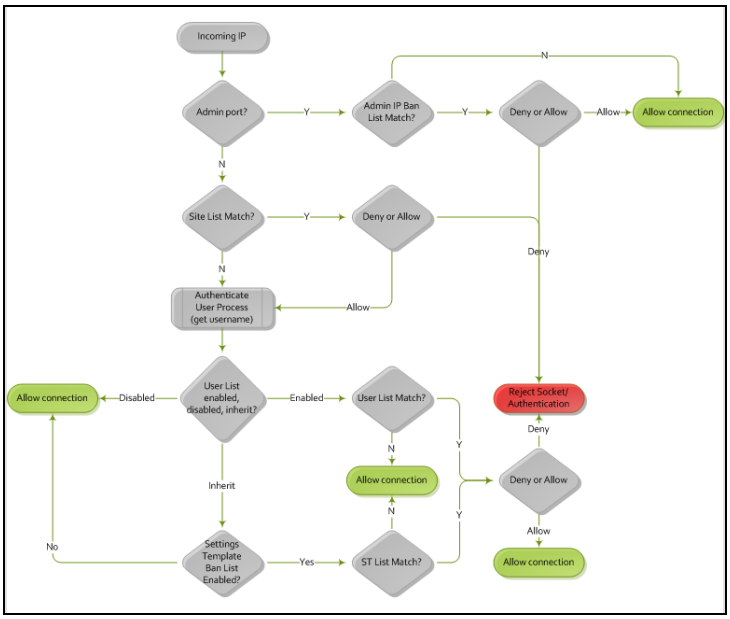
Controlling Access to the Site by IP Address

By default, all IP addresses are granted access to EFT. EFT allows you to grant access to only one specific IP address or a range of IP addresses, or deny access to one specific address or a range of addresses. EFT controls access on the Server, Site, Settings Template, and user account.

The IP access/ban list consists of a multiple, prioritized list of IP addresses, with each IP address designated as either allowed (whitelisted) or denied (blacklisted):

- EFT filters incoming IP addresses based on the IP address entries in the list, in order of precedence. The first "Deny" match on the list causes the filtering to cease Rule matching/parsing. If there is no match or no "Deny" for the Site list, the Rule will process against either the user list (if explicitly enabled) or against the Settings Template list (if user list is set to inherit).
- Any IP address allowed access is parsed against the Settings Template or user account IP address access/ban list upon user authentication.
    - If the user list is disabled, then no checking occurs.
    - If the user list is inherited, then the IP address is checked against the Settings Template list.
    - If the user list is enabled, then the IP address is checked against the user list only. See diagram below.
- All automatically banned IP addresses are maintained in a separate list, for both purposes of readability and for easier prioritization of all automatically banned IP addresses relevant to manually whitelisted or blacklisted IP addresses.
- You can unban more than one IP address at a time and search for specific IP addresses in the list.
- The **IP Auto-Ban**dialog box displays when and why an IP address was banned.

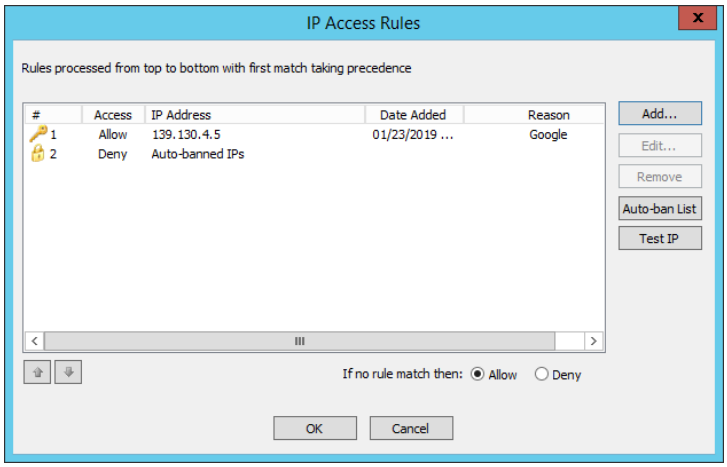
The diagram below provides a logic flow of EFT's IP address ban process.



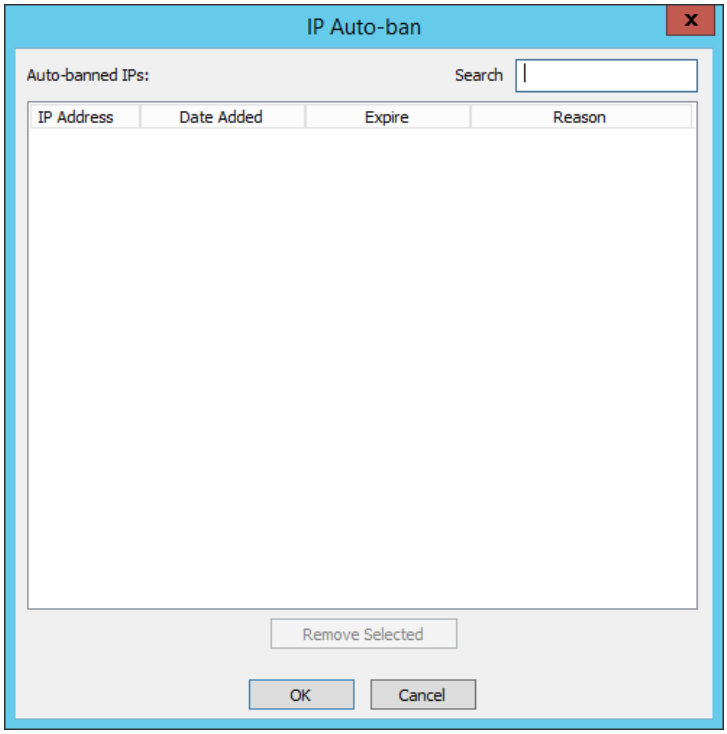
IP address policy changes are propagated to the DMZ Gateway whenever the policy is modified in the administration interface or by the auto-ban logic.

To grant/deny access by IP Address on a Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site, Settings Template, or user account, and then click the **Connections** tab.
3. In the **Network Usage and Security Settings** area, next to **IP access/ban list**, click **Configure**. The **IP Access Rules** dialog box appears.
    - **To add an IP address to the Rules**, click **Add**. Specify the IP address or mask, click whether to **Allow**or **Deny** the address, a **Reason** (optional), and then click **OK**. You can also specify a range of addresses. CIDR notation is supported for both IPv4 and IPv6 literals. For example: 001:cdba:9abc:5678::/64 for blocking an IPv6 LAN or 192.168.29.0/24 for an IPv4 network.



- **To remove a Rule**, click it in the list, and then click **Remove**. A confirmation prompt appears. Click **Yes**.
- **To edit a Rule**, click it in the list, and then click **Edit**. Edit the address, then click **OK**to save your edits.
- **To test whether an IP address is banned or allowed,** click **Test IP**. The **Test IP Connection**dialog box appears.
    - Provide an IP address to test, and then click **OK**. The **Result**(Allowed or Denied) and the **Reason**the IP is allowed or denied appear in the dialog box. Click **OK** to close the dialog box.
- **To view the list of banned IPs**, click **Autoban List**. **(On the Site only)**The **IP Auto-ban** dialog box appears.



The **Auto-banned IPs**Rule is defined by default. Any IP address that is banned automatically by the system is denied access, until an administrator removes it from the **Auto-ban List.**

- **To find an IP in the list**, type it in the **Search**box.
- **To sort the list**, click a column header.
- **To remove an IP from the list**, click it, and then click **Remove Selected**.
- The **Date Added** column displays the date and time the IP was added to the **Autoban List**, in MM/DD/YYYY hh:mm:ss AM/PM format.
- The **Reason**column displays the reason the IP address was banned (DoS/Flood prevention temporary ban, DoS/Flood prevention permanent ban, Invalid password attempts exceeded, Invalid username attempts exceeded, Too many consecutive invalid commands).
- Click **OK** to close the dialog box. The IP address/mask appears in the exceptions list.

4. Click **OK** to close the **IP Access Rules**dialog box.
5. Click **Apply**to save the changes on EFT.

For more information about how IP addresses are banned, refer to the topics below.

Related Topics

- Disconnecting Users after a Defined Number of Invalid Commands
- Banning an IP Address that Uses an Invalid AccountControlling IP Access for Remote administration
- Flooding and Denial of Service Prevention (Auto-ban)

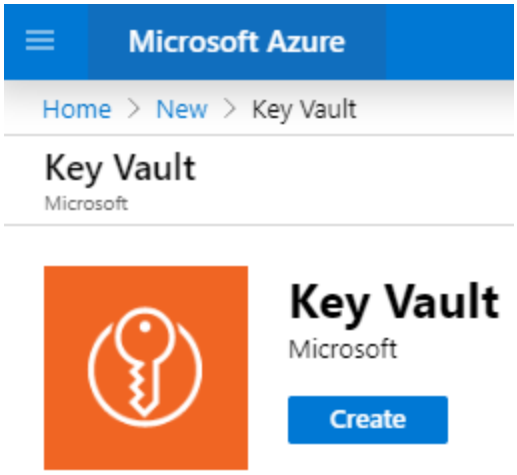
Configuring Azure Key Vault Support for EFT

This topic provide a *general* guideline to point you in the right direction to gather the necessary information to Configure the Secrets Module in EFT, which requires the Key Vault URL, Client ID, and Client Secret used to access the Azure Key Vault. This procedure assumes you already have an Azure account. (After you click **Create**on the **Key Vault** page (in the procedure below), you can sign in if you have an account, or you can create an account.)

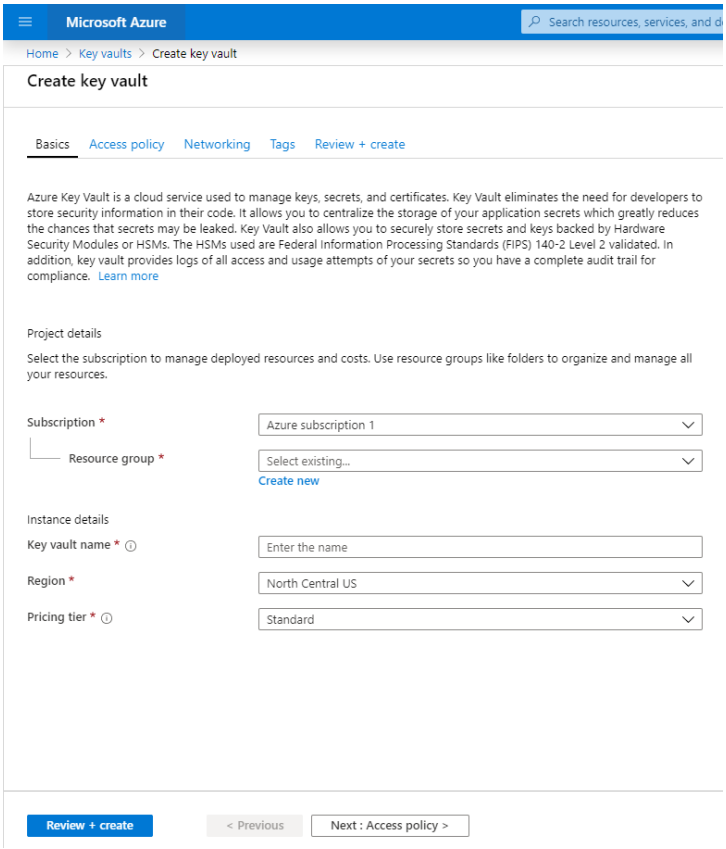
The knowledgebase article EFT Secrets: A Primer describes the various mechanisms used by EFT to protect its secrets and several frequently asked questions.

To configure Azure Key Vault support

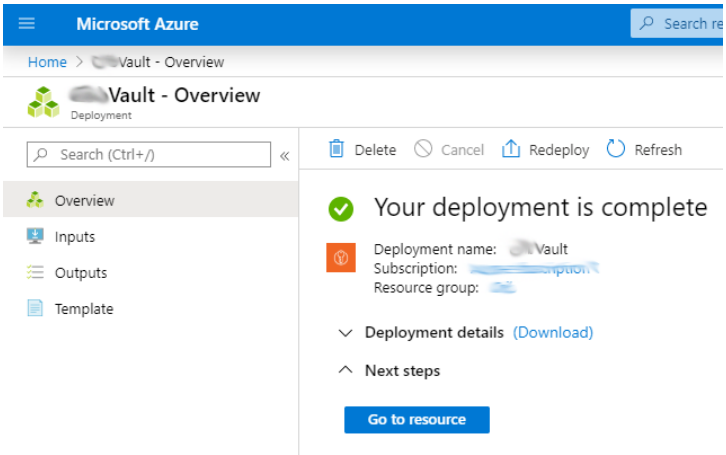
1. Sign in to the Azure portal at https://portal.azure.comand create a vault:
2. On the Azure portal menu or the **Home** page, click **Create a resource**.
3. In the **Search the Marketplace**box, type **Key Vault**., then click **Key Vault**.
4. On the **Key Vault** page, click **Create**.



5. On the **Create key vault** section provide the following information:
   - **Name**: A unique name is required.
   - **Subscription**: Choose a subscription.
   - Under **Resource Group**, click **Create new** and provide a resource group name.
   - In the **Region** pull-down menu, choose a location.
   - Leave the other options as their defaults.



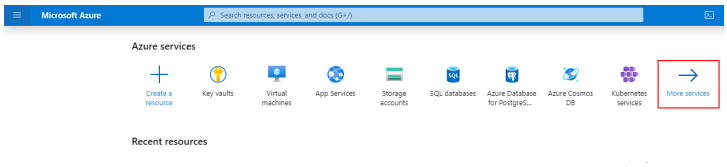
6. After providing the information above, click **Review and Create,** then click **Create**.



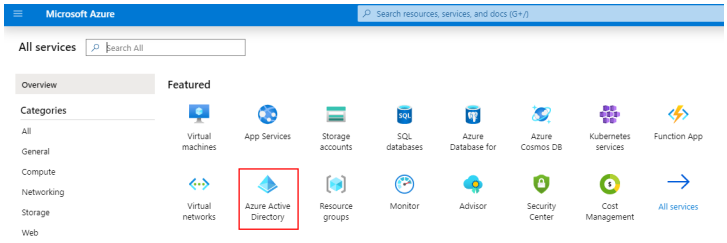
7. After **Your deployment is complete**appears, click **Go to resource**. You Key Vault information is displayed. (Take a screen shot and save it in a secure location.)

NEXT, you will need to create an application Client ID and Client Secret

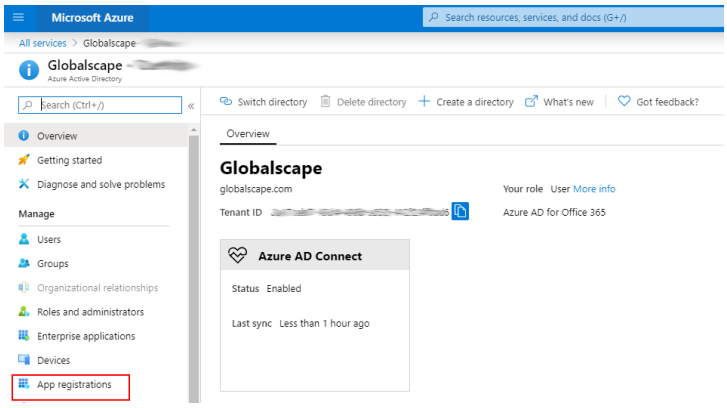
8. Under the main menu, click **Home**. The **Azure services** page appears.



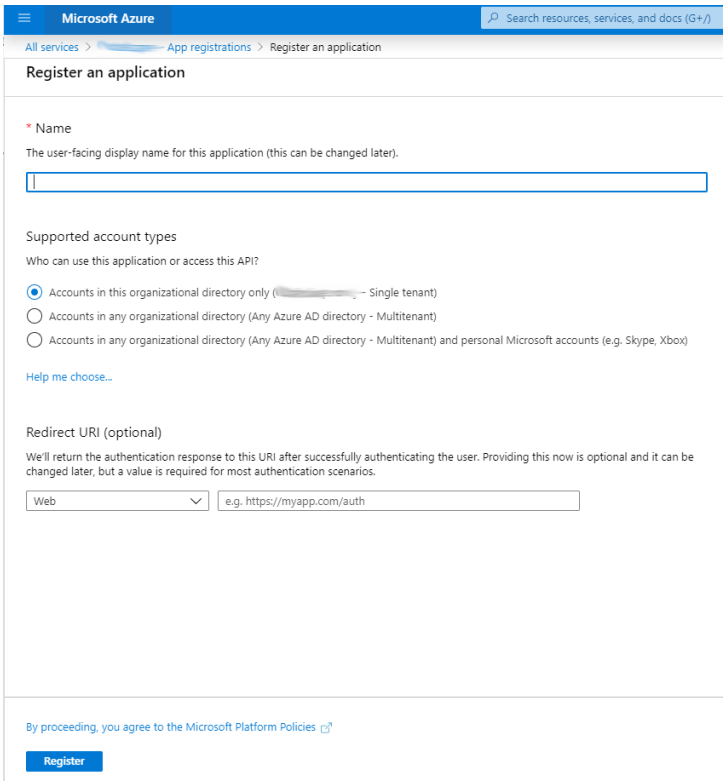
9. Click the **More services**arrow on the right.



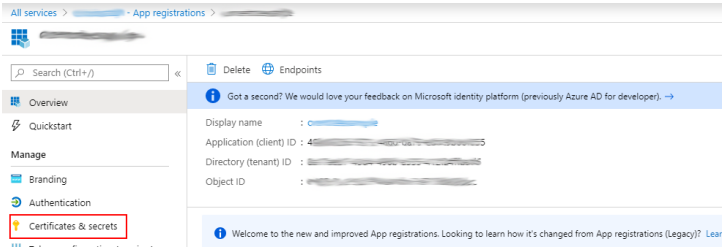
10. Click **Azure Active Directory** (Entra ID). (If your organization already has an Azure Active Directory (Entra ID) account, it will appear here, and you will need administration access to register your application (EFT).)



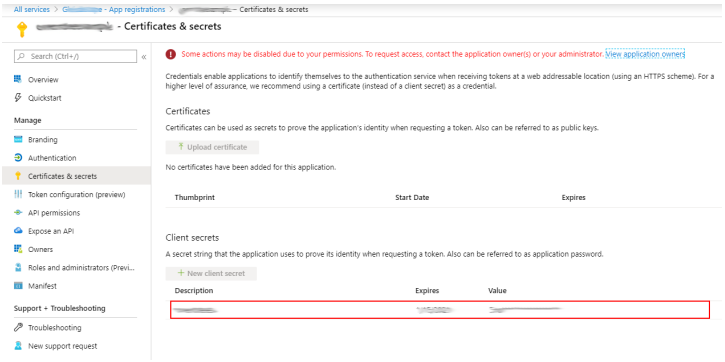
11. In the left pane, click **App registrations.**



12. Provide a name for the application (for example, eftTest), then click **Register**.



13. In the left pane, click **Certificates and secrets**.



14. Under **Client secrets**, click the icon to **Copy to clipboard**. (You must have permission/ be the application owner to do this.)

Related Topics

- Azure Data Lake Storage
- Configuring the Secrets Module
- Override VFS Credentials

Configuring the Secrets Module

The EFT Secrets module allows you to specify a storage location for passwords, authentication tokens, passphrases, and other security artifacts in use by the Site so that security and trust can be centralized. (Requires CCM.)

- The Azure Key Vault (AKV) functionality does not support proxies, so EFT must have direct access to Azure OR the server must reside in Azure.
- See the procedure belowfor what to do when a key or password changes in the AKV.
- EFT Secrets Primer (Knowledgebase)

> **NOTE:** If the Secrets module is enabled and CCM is not registered and the EFT trial expires, EFT will default to local storage to allow EFT administrators to continue to gain access to the site.

The Secrets module can store EFT passwords or other secrets it uses:

EFT Secrets	SQLite SiteConfig.<guid>.db location
AWS Connection Profile	ConnectionProfile table - Settings cell
Azure Connection Profile	ConnectionProfile table - Settings cell
Folder Monitor Override	EventRules table - Trigger cell
Event Rule passwords	EventRules table - Statements cell
SSH Key	SSHKey table - Password cell
SSL Certificate	Site table - Connections cell
ODBC Parameters	Site table - General cell
PGP key	Site table - Security cell
AS2	Client table - AS2 Outbound cell
Webservice	EventRules table - Statements cell
Proxy passwords	EventRules table - Statements cell
Override VFS credentials	Site table - General cell

You can specify:

- Store secrets in Azure Key Vault (AKV) via authentication token
- Store secrets in Azure Key Vault (AKV) via Managed Identities

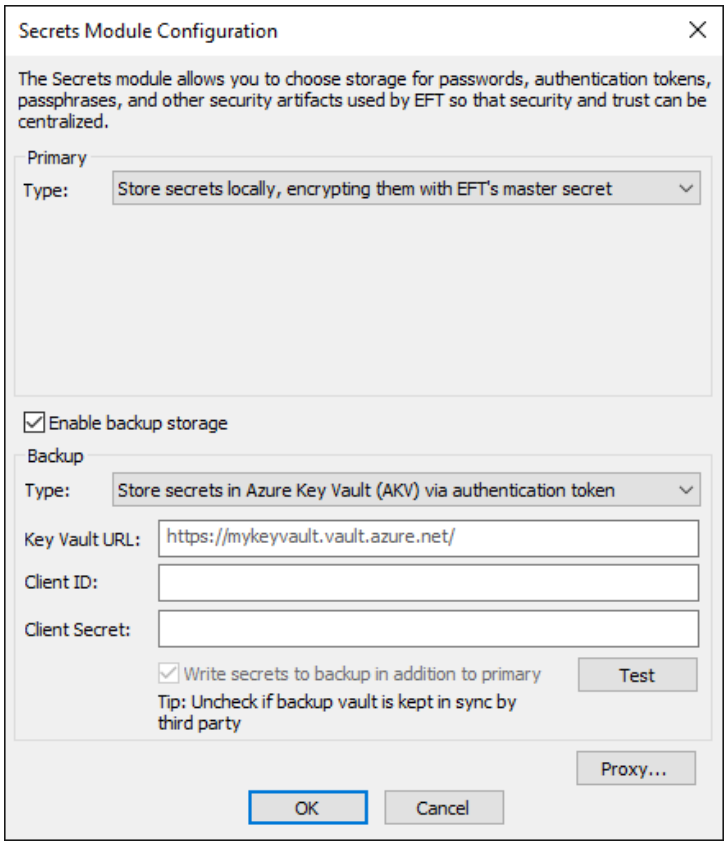
The Secrets module includes "hooks" into Azure Key Vault storage. When a secret is needed, EFT will request it from storage. When EFT is NOT hooked into a third-party

secure vault, it will use it's default security key to protect its Secrets module. An Azure secure token will be requested on startup and will be updated 5 minutes before it expires. When the Secrets module storage is changed, EFT gets secrets from current storage and saves them into new storage.

To configure the Secrets module

BEFORE PERFORMING THIS PROCEDURE, REFER TO CONFIGURING AZURE KEY VAULT SUPPORT FOR EFT TO CREATE THE CLIENT ID AND CLIENT SECRET.

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site, Settings Template, or user that you want to configure.
3. In the right pane, click the **Security** tab.
4. In the **Data Security** area, next to **Secrets module**, click **Configure**. The **Secrets Module Configuration** dialog box appears.



5. Select the **Enable backup storage** check box to backup secret storage. The backup options appear.
6. In the **Backup**area, click the **Type** drop-down list and select an option:

- **Store secrets in Azure Key Vault (AKV) via authentication token**
  - Provide the **Key Vault URL**, **Client ID**, and **Client Secret**used to access the Azure Key Vault.
- **Store secrets in Azure Key Vault (AKV) via Managed Identities**
  - Provide the Key Vault URL

7. The **Write secrets to backup in addition to primary** check box is selected by default. Clear the check box if you do not want to write secrets to backup or if the backup vault is kept in sync by a third party, such as Azure's vault backup. If the check box is not selected, EFT will not write to backup, but will attempt to read from the backup if the primary is unavailable, which may fail if the vaults are not kept in sync by the third party.
8. Click **Test**to ensure EFT can access the vault and that your Azure credentials are correct.
   - If you receive a **Connected failed** error message, verify your connection string, logon credentials, and that access to the Vault has been granted (if using managed identities).
9. Click **Proxy**to define a proxy server, if needed. (The Proxy applies to both the primary and the backup.)
10. Click **OK** to save the configuration, then click **Apply**on the **Security** tab.

What happens if the password/key in Azure is changed?

If you click **Test** and are presented with a connection failed error after it has been previously been connecting, it is likely that your Client Secret has expired.

DO NOT DELETE THE OLD SECRET UNTIL AFTER YOU CREATE A NEW ONE, AS SHOWN BELOW.

To allow EFT to connect to the key vault, EFT needs to be configuredin the Azure Key Vault under “App registration.” This is where the **Client ID** and **Client Secret** are generated. The secret is based off a client secret that will provide a value that is used in EFT. Azure’s App registration allows the client secret to expire in 1 or 2 years or never. An Azure administrator can create a new Client Secret as needed. If you have configured your secret to expire, set yourself a reminder to update the secret before it expires—EFT will not report an error that the AKV connection is failing.

The steps below are required to ensure EFT can connect to Azure AKV without issues when the client certificate is updated. The following procedure assumes that the App registration has already been created.

If the Client Secret has expired or been updated

1. Within Azure's Active Directory settings, click **App registrations**.
2. Click the EFT created registration app.
3. Click **Certificates & Secrets**.
4. Create a new client secret. (**Note**: Do not delete the old Client Secret until EFT connects to the new one!)
5. Save the new client secret value. (Copy it since it will be used in EFT.)
6. Login to the EFT administration interface.
7. On the **Site > Security**tab, next to **Secrets Module**, click **Config**.
8. Paste the new Client Secret (the value from step 5 above) into the **Client Secret** field.
9. Click **Test** to confirm the connection is successful.
10. Restart EFT and ensure you can still connect.
11. If connection was successful, delete the old Client Secret in Azure.

The following COM API property and enums are provided:

`SecretsModuleType`

- `SecretsModuleType_LocalPasswordsStorage,`
- `SecretsModuleType_AzureKeyVault,`
- `SecretsModuleType_AzureKeyVaultManagedIdentities`

The **ICISiteInterface** provides the following read-and-write properties:

- `SecretsModuleType`
- `SecretsModuleURL`
- `SecretsModuleClientID`
- `SecretsModuleClientSecret`

(Refer to the COM API documentation for more information.)

Deleting a Site

If you want to delete a Site that you no longer use, you can do so in the administration interface. When you delete a Site, the Site and the objects under it are deleted from the administration interface, but the folders in **C:\Inetpub\EFTRoot**, which includes Site and user folders, are not deleted. That is, if you were to create a new Site with the exact same name, it would be created with the same users.

If the Site folder (for example, C:\Inetpub\EFTRoot\MySite) is deleted, a warning message appears in the administration interface.

To delete a Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Site** that you want to delete, right-click it, and then click **Delete**. A password prompt appears.
3. In the **Password**box, type your EFT administrator password, and then press **ENTER**or click **Delete**. There is no confirmation dialog.

Enabling the Account Management Page

EFT provides an HTTPS account management page on which users can reset their password, if so configured in the administration interface.

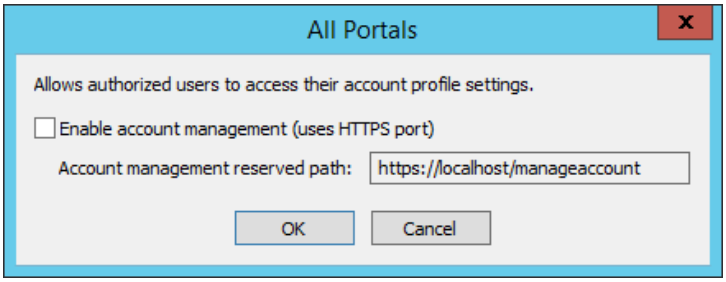
The account management page is hard-coded to https://<server-URL>**/manageaccount** with the default port of 443. If the HTTPS port is set to a different port, the user must provide the port number in the URL to log into the page (for example, **https://192.168.123.456/manageaccount:4433**).

It is ***strongly***recommended that you enable the account management page over HTTPS (using the procedure below) so that your users will be able to change their passwords. You must also enable HTTPS and SSLto use the account management page.

> **NOTE:** The account management page is not available when CAC is enabled.

To enable the account management page

1. In the EFT administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the **Site** that you want to configure.
3. In the right pane, click the Web tab.
4. Next to **Account management**, click **Configure**. The **All Portals** dialog box appears.



5. Select the **Enable account management page over HTTPS** check box. The **Account management reserve path** URL is displayed in the text box (for example, **https://localhost/manageaccount**). The URL is not editable, but you can select and copy it to provide to users.
6. Click **Apply**to save the changes on EFT.

When a user goes to the **https://<host>/managementaccount** page, they will be directed to the Web account login page, **//<host>/Web/Account/Login.htm**, and then the account management page appears. If the user is allowed to change their password, then the **Change Password for <user>** page appears. Otherwise, a message

appears that says the user does not have permission to change their password. This permission is enabled on the **Security** tab of the Site, Settings Template, and User account.

Folder Sharing (Workspaces)

(Requires HTTPS, Workspaces) The Workspaces feature of EFT allows end users to share their folders with other users. The user account that is sharing the folder maintains control of permissions to the shared folder, and can revoke sharing privileges at any time. Workspaces provides the ability to easily share and collaborate on information that is securely managed by EFT, including existing authentication, access control, auditing, governance, and Event Rule workflow capabilities available in EFT.

If an unsigned or otherwise invalid certificate is used in the Chrome browser, downloads will fail, even if you add the certificate to your trusted list. To resolve this issue, use a valid, signed certificate. Alternatives include:

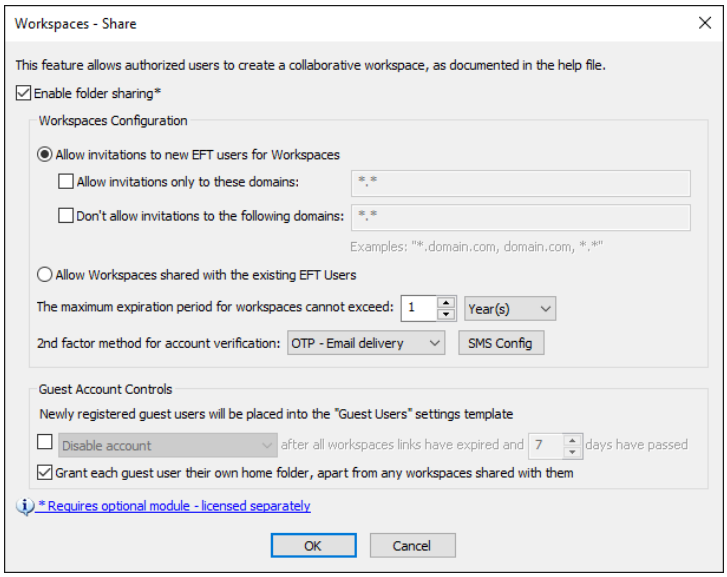
- Use a different browser
- Block downloads until you get a valid certificate
- Create a self-signed certificate outside of EFT, use a subject alternative name (SAN), then add the certificate to Chrome's trusted list.

Refer to Workspaces Licensesfor important information regarding Guest Accounts.

To enable Workspaces on the Site

(Refer to To enable Workspaces for a Settings Template or specific users below to disable/enable Workspaces for specific Settings Templates or users.)

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the Webtab.
4. Next to **Folder sharing**, click **Configure**. The **Workspaces - Share** dialog box appears.



5. Select the **Enable folder sharing** check box.
6. Under **Workspaces Configuration**, specify one of the following groups of users (any users or only existing EFT users) to whom users can send Workspaces invitations:
    - **Allow invitations to new EFT users for Workspaces**
        - (Optional) Select the**Allow invitations to these domains** check box, then specify the domains to which Workspaces users can send invitations, comma/semicolon delimited. Wildcards are supported (for example, *.domain.com or domain.com). The setting is not selected by default; that is, all domains *.* are allowed. (**Allow invitations to new EFT users for Workspaces** must be selected.) NOTE: Be sure wildcards are formatted correctly. That is, if you specify *.domain.com, then the domain www.domain.com is allowed.
        - (Optional) Select the **Don't allow invitations to the following domains** check box, then specify the domains for which you do not want to allow access to Workspaces. The field is comma/semicolon delimited; wildcards are supported (for example, *.domain.com or domain.com). The setting is not selected by default; that is, no domains *.* are blocked. NOTE: Be sure wildcards are formatted correctly. That is, if you specify *.domain.com, then the domain www.domain.com is blocked.
    - **Allow Workspaces shared with existing EFT users**
        - On an LDAP-authenticated Site, when a sender types a recipient email to share a Workspace, if that email does not belong to a local

(cached) account in EFT, EFT will extend its search to the LDAP authentication database.

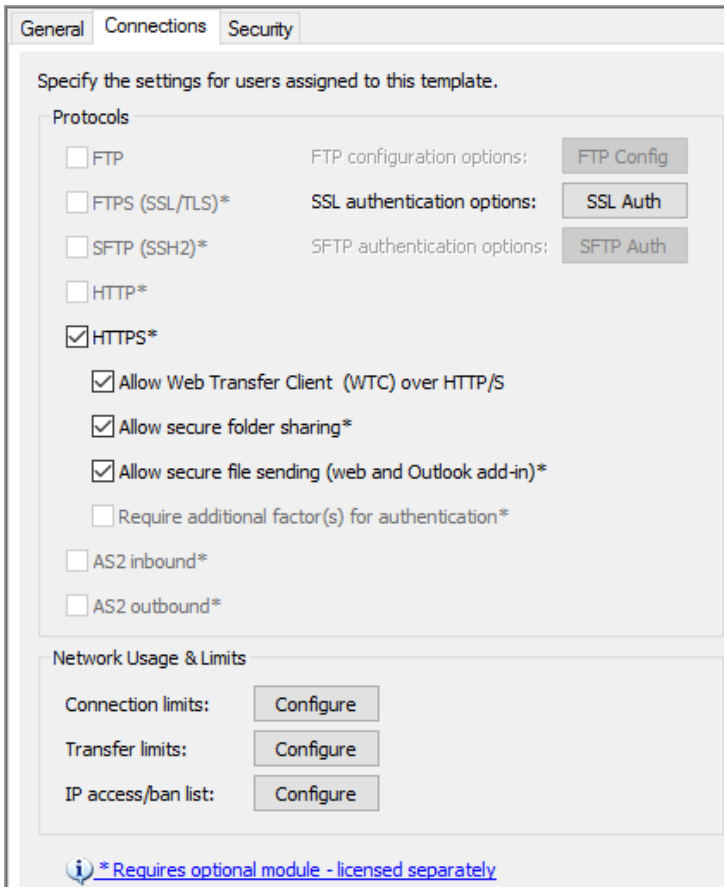
- Specify the **maximum expiration period** for a Workspace. Senders can set the expiration to happen sooner than what is defined on the server, but you cannot specify a longer period. (Refer to Enable Send Portal for information about retaining files after a Workspace link has expired.)
- Specify **2nd factor method** for account verification (OTP) options. Refer to Enable Multifactor Authenticationfor directions.

7. Under **Guest Account Controls**:
   - Specify whether to **Disable account**, **Remove account and home folder**, or **Remove account only**after all Workspaces links have expired and *n*days have passed. When set to 0 days, the account(s) will be cleaned up at midnight. If the Guest account is disabled, the user will not be able to log in unless the EFT administrator enables or removes the account (and then the guest user would have to recreate their account). Refer to Workspaces Invitations for an example of using the **User Account** action to enable an expired Guest account.
   - To grant guest users their own home folder, select the **Grant each guest user their own folder** check box. Selecting the check box prevents guests from viewing other files in the Workspace's home folder.

     If the check box is ***not***selected, the user has:
     - Read-only access to home folder.
     - List view of Workspaces with permissions as allowed by Workspaces owner, regardless of any protocols used to access the account.
8. Click **Apply**to save the settings.

To enable Workspaces for a Settings Template or specific users

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Settings Template or user account.
3. In the right pane, click the **Connections**tab.



4. In the **Protocols** area, select the **Allow secure folder sharing**check box. If this check box is not available, you have not activated the Workspaces licenses or the trial has expired; or you have not enabled Workspaces for the Site.

   HTTPS must also be enabled.

5. To also allow secure file sending in the WTC and in the Outlook add-in, ensure that the **Allow secure file sending** check box is selected.
6. (Optional) To enable additional authentication by email or SMS, select the **Require additional factor(s) for authentication** check box.
7. Click **Apply**.

Related Topics

- Enable Multifactor Authentication for the WTC
- Workspaces SSO Authentication
- Guest Users
- Workspaces
- Sharing Folders

- Workspaces Activity Report
- Workspaces for Outlook

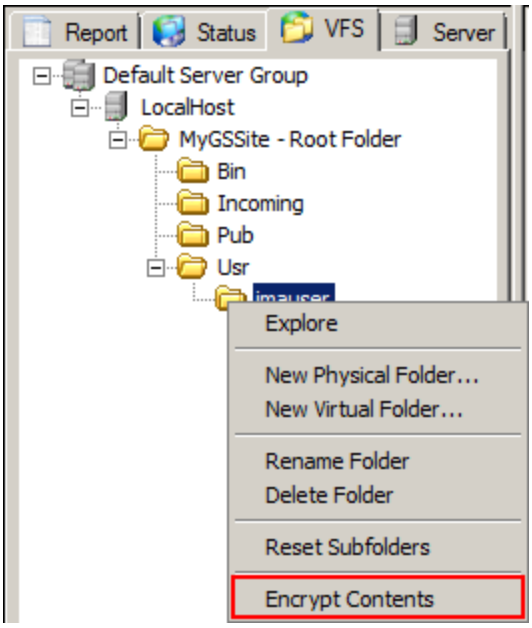
EFS Encryption

Physical folders stored on the disk in EFT's Virtual File System (VFS) can be transparently encrypted during read/write using Microsoft's Encrypting File System (EFS) by which data is encrypted as it is written to disk, and decrypted prior to transmission.

- Before you enable this feature, it is recommended that you set up appropriate backup measures to protect your data. If you need to recover a private key to decrypt data, and that key is lost, you will not be able to recover the data that the key protects. If you need more information on setting up appropriate backup procedures, refer to Configuration and Security Best Practices.
- When EFT is running in HA mode and sharing a network resource, you must run the EFT server service with a Log On account that can access that shared network resource.
- EFS is not available for systems running on FAT32 file systems. NTFS is required.
- EFS is not available with NT authentication due to limitations of NT authentication. If you require this feature with an NT set up, LDAP authentication is recommended.
- The PCI DSS requires that logical access and decryption keys be managed independently for disk-level encryption. If you enable this EFS for a high security-enabled Site, EFT prompts you to disable it, or continue with reason.
- The PCI DSS requires that if EFT disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts. That does not mean EFS cannot be used at all, but rather that it cannot be used as the sole mechanism for repository encryption. For this reason, the Server will only warn, rather than fail, during an audit.
- If you have a large number of VFS folders and the interface becomes unresponsive when EFS is enabled, be sure to clear the EFS folder icon check box. Selecting the **Enable EFS folder icons**check box when you have a large number of VFS folders can cause the interface to become unresponsive while the server checks each one for encrypted contents.
- You cannot have the folder open when trying to encrypt the folder in EFT.

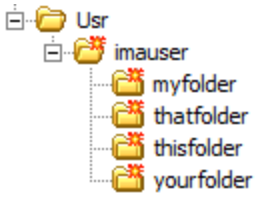
To enable EFS encryption

1. In the administration interface, connect to EFT and click the **VFS**tab.
2. In the left pane, right-click the parent folder you want to configure, and then click **Encrypt Contents**.



3. If the folder you selected has subfolders, a confirmation message appears.

4. Specify whether to **Apply changes to this folder only** or **Apply changes to this folder and all subfolders**, and then click **OK**.
   - If the Enable EFS folder icons check box is selected, the encrypted folder and subfolders display a red asterisk to indicate that the folder contents are encrypted.



5. To remove encryption, right-click the encrypted folder and click **Encrypt Contents**to clear the check box.

6. If the folder you selected has subfolders, a confirmation message appears. Specify whether to **Apply changes to this folder only** or **Apply changes to this folder and all subfolders**, and then click **OK**.

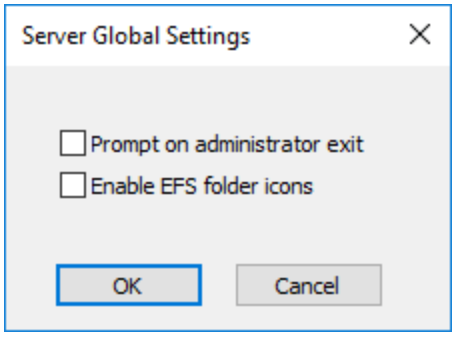
Enable EFS Folder Icons

When EFS is applied to a folder, you can configure the Server to add a red asterisk to the folder icon to indicate that the folder contents are encrypted. This setting is turned off by default. If you select the **Enable EFS folder icons** check box, the server will check each folder for encrypted contents before displaying the icon.

If you have thousands of folders, you should leave the check box unselected; selecting the check box when you have a large number of folders can cause the interface to become unresponsive while the server checks each one for encrypted contents.

To enable the EFS folder icons

1. On the main menu, click **Edit > Global Settings**.



2. Select the **Enable EFS folder icons** check box.
3. Click **OK**. (To disable the feature, clear the check box.)

Related Topic

- Encrypted Folders (EFT Encryption) with EFT-managed encryption

Encrypted Folders (EFT Encryption)

EFT Server provides the following forms of securing files on disk (data-at-rest encryption):

- OpenPGP-based encryption is a well-known, dual-key based encryption technology. The primary benefit is the fact that only recipients whose public key was included at the time of encryption will be able to decrypt the file, assuming they own the corresponding private key to their public one. This provides more control over who can access the data, vs. other methods. PGP has two shortcomings: First, it requires that participants create and maintain their key pairs, adding complexity to the process. Second, it is not a streaming encryption technology, as the entire file must be present (written to disk) before encryption (or decryption) can occur. In the context of file transfers, the result is temporary files that cause havoc with automation that consumes files the moment they are received in the target directory. Refer to OpenPGP and EFT for how to use OpenPGP.
- Integrated Windows encryption via Encrypted File Share (EFS) addresses all of the drawbacks of PGP, eliminating participant key management and providing streaming encryption at the file I/O level; however, it also suffers from two shortcomings: First, some network drive technologies do not support Windows EFS (turning it on in EFT has no effect). Second, standards such as PCI DSS disallow the use of encryption technologies where the keys required for encryption/decryption reside on the systems within PCI scope. It just so happens that Window's EFS keys do reside on the target system. Refer to Enable EFS Encryption for how to use Windows EFS integration.
- Encrypted folders(EFT built-in encryption) provides an alternative to using a best-of-breed 3rd party data-at-rest encryption solution. EFT's encrypted folders provide streaming encryption (and decryption), enabling transparent, seamless file read/write. The symmetric encryption leverages AES 256 in CTR mode, with the encryption key known only to EFT. Any file touched by EFT's protocols (either as a server or as a client) are automatically encrypted (or decrypted) on arrival or departure, as appropriate. In SSL FIPS mode, encryption at rest uses the FIPS-certified SSL library.

  The primary drawback to the built-in encryption feature is that fact that any side-channeled files, such as those directly copied into a folder designated as an encrypted folder, will not be encrypted or decrypted by EFT. In fact, if you place a plaintext file in an encrypted folder and a customer logs in and downloads the file, the file will be corrupted, as EFT will attempt to decrypt what it thinks is an encrypted file. This risk can be mitigated by never side-channeling

files into folders designated as secure. Instead, use EFT's event rule Copy/Move-> LAN copy action to move files from network shares or physical folders into the secure target, as that will result in the content being encrypted (or decrypted, if done in the other direction).

> **NOTE:** Encrypted folders with long paths are not supported. (TFS389235)

- **Encrypted Folders Command-Line Utility** - EFT's built-in folder encryption feature will encrypt files as they arrive or decrypt them as they leave EFT via standard protocols; however, there may be instances where you need to encrypt or decrypt files independent of EFT, while adhering to the same encryption mechanisms (AES-256 symmetric-key). For example, you may want to encrypt a file received by a folder monitor rule, or conditionally encrypt files prior to emailing them, or decrypt previously encrypted files side-channeled into EFT from a different EFT server. To that effect, EFT's encryption/decryption subroutines have been exported to a command utility, **eftencrypt.exe**, which is installed alongside EFT in the **\Redistributables** subfolder. You can run the utility directly or from within EFT's Event Rules, by leveraging the built-in PowerShell action. You can also copy the utility to another computer to encrypt and decrypt files there. (The utility follows standard command line rules.)

To use the eftencrypt.exe utility

1. Locate the **eftencrypt.exe** utility. (The default is **C:\Program Files\Globalscape\EFT Server**)
2. Locate your Site or specific Encrypted Folder's encryption key. Alternatively, create a new 256-bit key (64 hexadecimal characters, i.e. 32 bytes in length).
3. Locate the name of the target file you want to encrypt or decrypt.
4. Launch a command line prompt or PowerShell, running as Administrator. Alternatively, create a PowerShell action in EFT's event rules.
5. To encrypt or decrypt in place, type: eftencrypt.exe <key> <path to target file>
6. To encrypt or decrypt using source and destination: eftencrypt.exe <key> <path to source file> <path to target file>

Each of these methods has benefits and drawbacks. Other alternatives include using third-party data-at-rest encryption, such as the built-in encryption provided by some NAS devices.

EFT provides an advanced property, **IgnoreEncryptedFoldersInOutboundTransfers**, which can be used to prevent EFT from decrypting encrypted folders during transfers. For example, EFT receives a file into an encrypted folder and EFT encrypts it. Then the file is transferred to another system using EFT's "Copy/Move" event rule action, which normally results in the file being decrypted. If the advanced property **IgnoreEncryptedFoldersInOutboundTransfers** is set to True, the file will remain encrypted when transferred. It can then can be decrypted later with the **eftencrypt.exe** utility.

EFT Built-In Encrypted Folders

Physical folders can be transparently encrypted during read/write using EFT-managed AES-256 *symmetric encryption* (CTR mode), which uses a secret key known only to the server. The server will encrypt files as they arrive over supported protocols, and decrypt files when departing over those same protocols. The server, when acting as a client, will also encrypt files that it downloads into an encrypted folder, and decrypt files that it copies or moves to a remote server, including LAN copy. (See below for instructions for creating the key.)

- EFT randomly generates the Encrypted Folders key upon new Site creation. You should change the secret and maintain a copy of the secret in your key manager.
- If the Advanced Property **EncryptedFolderKey**is defined and not malformed, EFT uses it for encryption/decryption, read at service startup. (This is mainly for EFT upgrades to 8.0.4 from earlier builds. The key can be created/edited in the **Encrypted folders** dialog box, as described below.)

- Upon EFT upgrade, EFT generates a new key if the key is the old "default" value, and no other key is defined
- Per-folder encryption keys can be used to encrypt the contents of all data in the site root automatically, using a separate key for each sub-folder off of the site root, and also for folders referenced by virtual folders (VFS) that are shared by users.

The following considerations for encrypted folder targets should be noted:

- Encrypted folders are limited to physical folders (Per-folder encryption keys can be used on physical folders referenced by virtual folders.)
- Encrypted folders affect subfolders within the designated folder
- Encrypted folders can only point to folders that are under the Site root (for example, **C:\InetPub\EFTRoot\MySite**)
- When using Encrypted folders, you can only encrypt files in the directory hierarchy of the Site's root folder. Make sure that the Site root folder on the **Site > General** tab is pointing to the correct path. That is, if the HA config drive is **D:\HAConfig\,** you should edit the Site root folder to point to **D:\HAConfig\InetPub\EFTRoot\MySite**.
- Encrypted folders cannot be EFT system folders (Install Folder, App Data Folder, Cluster Share) and Windows reserved directories (Windows, ProgramData, ProgramFiles, ProgramFilesx86), or their parents or children, and cannot be specified even by server administrators. This is includes subfolders of those folders.
- When configuring network shares for data encryption, the EFT service account must have access to the encrypted folder path; otherwise, you will be presented with a failure
- Using the CIC Action with encrypted files will not return an accurate result. Copy/move the files to a folder that is not encrypted to process with the ICAP server.
- If you are remotely connected via the administration interface, you will not be able to browse for folders. Instead, you must specify a valid, approved path, local to the server.
- Whether local or remotely connected via the administration interface, administrator accounts beneath the role of Server administrator (that is, Site administrator and below) will not able to browse for folders. Instead, these administrators must specify a valid, approved path, local to the server.
- If the server cannot perform initial encryption or final decryption due to lack of permissions, sharing violations, or network disconnect, a warning will appear indicating that "Some files in the folder were not [encrypted|decrypted]. The data in the folder might be corrupt."

- The following protocols and protocol commands are encryption/decryption aware:
  - EFT FTP/HTTP/SFTP Server (Listening Engines): all operations: upload, download, resume, FTP COMB, FTP and HTTP XCRC32, HTTP Copy file, HTTP/FTP/SFTP move file/folder, HTTP ZIP Folder Download.
  - EFT FTP/HTTP/SFTP/Local Transfer Client (Client FTP transfers): offload, download, resume, Pre/Post commands, "Rename To" after download, FTP data integrity check (CRC).
- All side-channel operations and all actions outside of copy/move/download are unaware of encryption/decryption. So if, for example, you have a Timer rule that downloads a file from a remote host, to an encrypted folder, and then a subsequent action attempts to manipulate that file (for example in Advanced Workflows), that file could be encrypted, and thus Advanced Workflows will not be able to parse it.
- A new logger is available in Logging.cfg for output to EFT.log, labeled EncryptedFolders, set to TRACE by default.
- COM support is available
- You can only encrypt the folders in the Site's root folder. If you attempt to encrypt folders outside of the EFT Site's root folder (for example, C:\InetPub\EFTRoot\MySite) an error prompt occurs: "This folder is not in the directory hierarchy of this Site's root folder."
- EFT system folders (Globalscape/EFT, AppData, and cluster share) and Windows reserved directories (Windows, ProgramData, ProgramFiles, ProgramFilesx86), as well as their parents or children, cannot be encrypted. If a reserved path is selected in the**Folder to Encrypt** dialog box, an error prompt occurs: "This is a reserved path and cannot be encrypted."
- Before you enable this feature, it is recommended that you set up appropriate backup measures to protect your data. If you need to recover a private key to decrypt data, and that key is lost, you will not be able to recover the data that the key protects. If you need more information on setting up appropriate backup procedures, refer to Configuration and Security Best Practices.
- If you had used the Encrypted Folder Key advanced property in versions prior to v8.0.4, the property for the key will appear in the AdvancedProperties.json file. EFT only uses that advanced property for backwards compatibility. After upgrading, if you want to change the key you should do so in the EFT administrator interface, NOT via the advanced property.
- The following scenarios represent the only way in which files get ENCRYPTED when interacting with an encrypted folder:

    - When files are uploaded to EFT via HTTP/FTP/SFTP into an encrypted folder.
    - When files are downloaded by EFT (via a download action) via all protocols including LAN, from a remote server into an encrypted folder.
        - Likewise when using EFT's synchronize action (make local just like the remote), when downloading to an encrypted folder.
    - When PGP action writes file to an encrypted folder. The file is first PGP encrypted then AES-256 encrypted in a streaming fashion.
- The following scenarios represent the only way in which files get DECRYPTED when interacting with an encrypted folder:
    - When files are downloaded from EFT via HTTP/FTP/SFTP. The file is decrypted before it is sent down the wire.
    - When files are uploaded (offloaded) by EFT (via copy/move action) via all protocols including LAN, to a remote server.
        - Likewise when using synchronize action (make remote appear as local), when uploading from an encrypted folder.
    - When PGP action reads a file from an encrypted folder. The file is first AES-256 decrypted, then PGP decrypted in a streaming fashion.
- The advanced property **IgnoreEncryptedFoldersInOutboundTransfers** is used to prevent EFT from decrypting encrypted folders during transfers. For example, EFT receives a file into an encrypted folder and EFT encrypts it. Then the file is transferred to another system. If the advanced property **IgnoreEncryptedFoldersInOutboundTransfers** is true, the file remains encrypted when transferred. It can then can be decrypted with eftencrypt.exe. Use eftencrypt.exe <key> <path to target file> to run the decryption process, and then file is decrypted.

Site Encryption

You can encrypt all folders under the Site root using a single, reusable key for encrypting and decrypting data. EFT will encrypt all data in that folder and its subs using the Site encryption key. Subsequent files written to those folders by users uploading files will result in those files being encrypted with the site encryption key automatically and transparently. Event Rules that process files written into those folders will decrypt using the site encryption key. (Refer to Enabling EFT-Managed Encryption, below.)

Per-Folder Encryption

If you want to encrypt the contents of all data in the Site root, you can use a separate key for each sub-folder under the Site root, and also for physical folders pointed to by virtual folders (VFS) that are shared by users.

1. In the **Folder to encrypt** dialog box, add each sub-folder under the Site root folder, and then assign it a per-folder encryption key, as described in Enabling EFT-Managed Encryption, below. For example:
2. EFT encrypts all data in the specified folders and sub-folders using the corresponding folder encryption key.
3. Subsequent files uploaded to those folders by users will be encrypted with the corresponding folder encryption key.
4. Event Rules that process files written into those folders will decrypt the files using the folder encryption key.

User-Specific Encryption

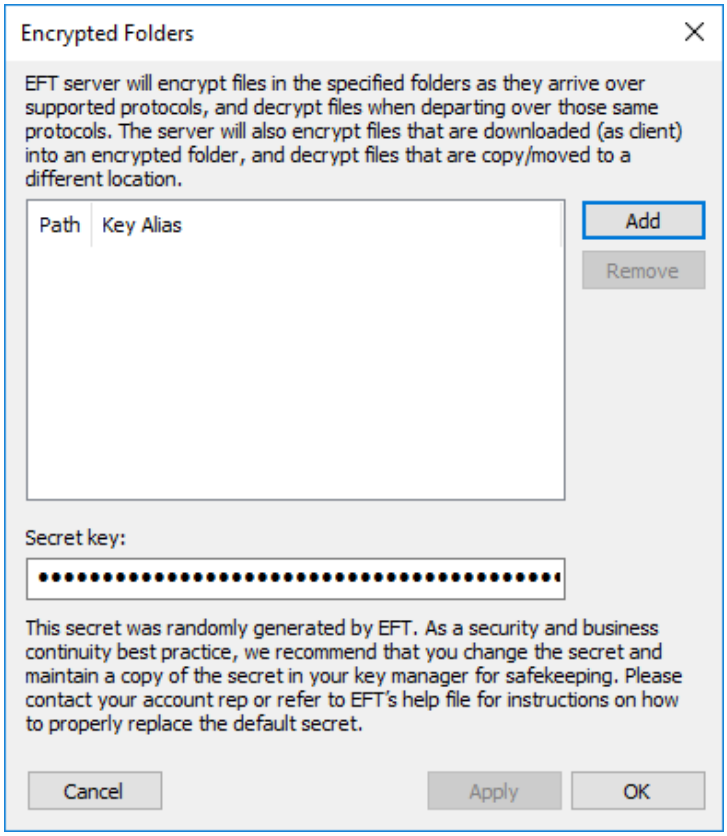
If you want to encrypt the contents of all data in the Site root, and also want to use a user-specific encryption key.

1. In the **Folder to encrypt** dialog box, click the folder icon to select a user's home folder.
2. Click **Use unique encryption** key and provide a key from the user's password manager.
3. **Click** OK.
4. EFT will encrypt all data currently in that folder and its sub-folders, including any physical folders pointed to by virtual folders, using the corresponding folder encryption key.
5. Subsequent files written to those folders by users uploading files will result in those files being encrypted with the corresponding folder encryption key.
6. Subsequent physical folders added by the user or admin or physical folders added by nature of a new virtual folder being associated with that user will results in their newly added contents also being encrypted.
7. Event Rules that process files written into those folders will decrypt using the corresponding user encryption key.

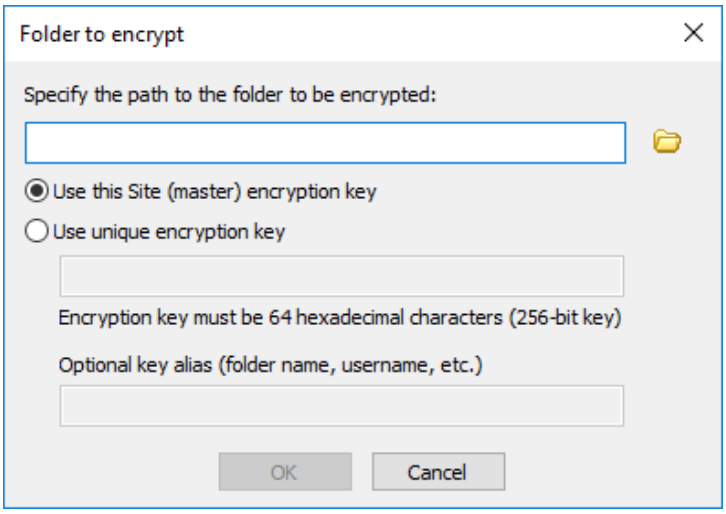
Enabling EFT-Managed Encryption

To enable EFT-managed encryption

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Security** tab.
4. In the **Data Security** area, next to **Encrypted folders**, click **Configure**. The **Encrypted Folders** dialog box appears.



   - Set the value to a string of exactly 64 hexadecimal digits (that is, 0-9 and A-F)
   - This value is not used if the value is blank or malformed (for example, if you have more or less than 64 digits)
   - Restart the EFT server service for the new key to take effect.
   - In an HA or Disaster Recovery scenario, each EFT must share the same key.
5. To add folders that contain files you want to encrypt, click **Add**. The **Folder to encrypt** dialog box appears.



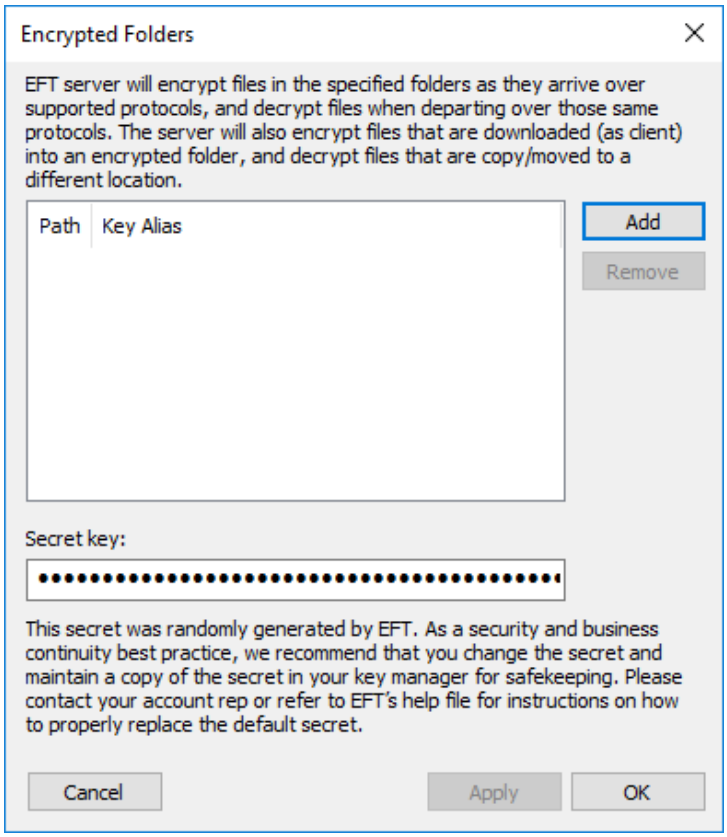
6. Type or browse for the folder that you want to encrypt. You can only encrypt the folders in the Site's root folder (for example, C:\InetPub\EFTRoot\MySite). (See note above regarding clusters.)
7. Click one of the following:
   - **For the Site encryption key**, click **Use this Site (master) encryption key** (the default).
   - **For per-folder encryption**, click **Use unique encryption key**, then paste or type the key (64 hexadecimal characters, 256-bit key). Optionally, provide an alias for this key. Note that using the same alias more than once does not cause a prompt, warning, or error. You can provide anything you want as an alias. The alias is purely for you to identify keys. If you want to use the same alias or no alias, you can. (However, providing the same alias for more than one key defeats the purpose of providing the alias.)

   Files uploaded to this folder will be encrypted upon arrival and decrypted upon departure over EFT's supported protocols. EFT will also encrypt files that are downloaded (as client) into an encrypted folder, and decrypt files that are copied or moved to a different location.

   EFT will attempt to decrypt any and all files already present in the folder. (This may take a long time if there are many files in the folder.)

To remove or replace an encrypted folder from the list

1. On the **Site > Security**tab, click **Configure** next to **Encrypted folders**. The **Encrypted Folders** dialog box appears.



- If the **Folder Path**list is empty, then the password field is NOT read only (that is, you can change the key).
- If the **Folder Path**list is NOT empty, select a folder in the list of folders, then click **Remove**. All encrypted files in the "removed" folder will be decrypted. (This may take a long time if there are many files in the folder. Note that files are not deleted, just unencrypted.)

2. In the **Secret key** box, provide a new key, then add the folder(s) back to the dialog box to be encrypted.
3. Click **OK** to close the dialog box, then click **Apply**.

Related Topics

- Personal Data Encryption
- Privacy Configuration

Flooding and Denial of Service Prevention

EFT provides a built-in system to detect and counter against various layer-7 targeted DoS attacks. These attacks either intentionally target availability or do so indirectly as a byproduct of brute forcing, vulnerability scanning, directory traversal, and similar attacks that attempts to exploit confidentiality or integrity. EFT uses a point system to determine the likelihood of an attack, with separate counters in place to account for different attack vectors. You can control the sensitivity of the attack detection logic or override the default values, if desired.

Other Attack Types and their Prevention

To mitigate the effects of Layer 3 or 4 DoS attacks, including volumetric Distributed Denial of Service (DDoS) attacks, we recommend the use of external DDoS protection services, where traffic is redirected to a content delivery network cloud security provider, which in turn returns only clean traffic to your organization. These solutions can be costly, but are the only effective means of preventing these types of attacks.

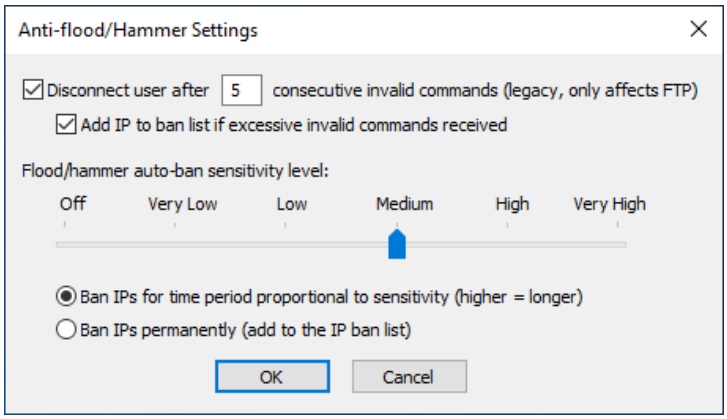
Apart from the availability protections mentioned on this page, EFT includes additional protections against confidentiality and integrity attacks. Some of those are configurable, such as failed login attempt ban logic, password complexity rules, username blacklisting, IP white/blacklisting, banned file types, max allowed connections from same IP, and various other configurable settings. EFT also includes numerous internal protections against typical attacks as documented by OWASP, including, but not limited to:

- Performing input and resource request validation, cleaning, and escaping
- Applying best practices to session creation, management, destruction
- Proper application of ACLs for resource authorization
- Internal protections against XSS, CSRF, and similar attacks

These protections and more are covered in other sections of the guide or in knowledgebase articles in more detail.

To enable flood and DoS prevention and set the sensitivity value

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the node of the Site you want to configure.
3. In the right pane, click the **Connections**tab.
4. In the **Network Usage and Security Settings** area, next to **Denial of Service settings**, click **Configure**. The **Anti-Flood/Hammer Settings**dialog box appears.



5. In the **Flood/hammer auto-ban sensitivity level** area, specify a sensitivity level using the slider bar.

   If you set the slider to **Off**, **Very Low**, or **Low** on a high-security-enabled Site, a message appears to warn you that this setting violates PCI DSS requirements related to securely configuring cardholder environments.

6. Click a ban period:
   - **Ban IPs for time period proportional to sensitivity (higher = longer)**
   - **Ban IPs permanently (add to TCP/IP access restrictions list)**
7. Click **OK** to close the dialog box.
8. Click **Apply**to save the changes on EFT.

> **NOTE:** Temporarily banned IPs are not stored in the database. They are kept in runtime memory. They are also node-specific.

See also Disconnecting Users after a Defined Number of Invalid Commands and Controlling Access to the Site by IP Address.

Flood and DoS Prevention Scoring

Behind the scenes, EFT applies several counters that it uses to identify possible attacks. If an attack is identified, the attackers IP is banned for a time proportionate to the sensitivity level. High sensitivity levels offer greater protection but may also result in a higher number of false positives. We recommend starting at the Medium sensitivity level, and then adjusting the slider over time as you analyze traffic patterns and characteristics.

Socket connections

This counter applies to any socket connection made with EFT's listener ports and is useful for countering everything from malicious and intentional SYN floods to

innocent but damaging misconfiguration by partners hammering your server in a misguided attempt to determine availability.

How it works: Using the Medium sensitivity value as an example, EFT sets a 1,000-point limit or threshold that must not be exceeded for a given duration of time, called a timer tick, which equates to a period of 10 seconds. Starting at zero points, each new socket connection made from the same IP address to a non-HTTP port will add 100 points to the prior value. This means that 10 connections in rapid succession (within 10 seconds) to a non-HTTP port would result in a short-term ban. Connections made to HTTP ports only accumulate 8 points at a time, to accommodate for the typical higher number of requests associated with HTTP, thus allowing up to 125 connections from the same IP during that same 10-second duration. This may seem high, but a typical HTTP pre-session behavior may yield upwards of 40-50 different requests (loading login page and various public assets, then link to lost password or other portals).

At each 10-second timer tick, the accumulated points are reduced by 350 points, effectively bringing the counter back to 0 in a little over 30 seconds (-350 points per timer tick is equal to -1050 points after three ticks), assuming no additional connections are made. If an IP exceeds the connection-points limit and is banned, it will be unbanned once the points fall back to zero. At a 35-point reduction per timer ticket, it would take roughly 30 minutes for that to occur.

> **NOTE:** You can also elect to ban IPs permanently vs. temporarily, but we do not recommend this as IP assignment can change over time and you don't want to accidentally block an IP from which legitimate traffic may arrive in the future.

Below is the table for socket connections at each sensitivity level. + points are added and - points reduced from the accumulated points.

Security Level Characteristics – Global (IP) Counter	Protocol	Very Low	Low	Medium	High	Very High
Starting points	All	0	0	0	0	0
Point limit	All	2000	1500	1000	800	600
+ Points for each socket connection	HTTP	8	8	8	8	8
+ Points for each socket connection	FTP, SFTP	100	100	100	100	100
- Points at each timer tick (approximately every 10 seconds)	All	(2000)	(750)	(350)	(300)	(150)
- Points at each timer tick if IP has been banned (exceeded limit)	All	(200)	(75)	(35)	(30)	(15)

FTP and SFTP session flood

Security Level Characteristics – Global (IP) Counter	User	Very Low	Low	Medium	High	Very High
Starting points	Any	0	0	0	0	0
Point limit	Any	2000	1500	1000	800	600
+ Points for each valid command	Any	10	10	10	10	10
+ Points for each invalid command	Any	300	300	300	300	300
- Points for each session clean exit	Any	(All)	(All)	(All)	(All)	(All)
- Points at each timer tick (approximately every 10 seconds)	Any	(2000)	(750)	(350)	(300)	(150)
- Points at each timer tick if IP has been banned (exceeded limit)	Any	(200)	(75)	(35)	(30)	(15)

HTTP session flood

HTTP/S session counters are a bit more nuanced, as there are requests that may occur both anonymously and as part of an authenticated session. The User column in the table below distinguishes between these two cases. Commands are HTTP verbs, whereas Path is the resource referenced by that verb. For example, a non-authenticated request to get a non-existent resource (perhaps a directory traversal probe) would accumulate 150 points, whereas the same request by an authenticated user would result in zero additional points. In addition to the base scores, administrators can optionally designate blacklisted or whitelisted resources (paths). A blacklisted path can be used to perform an immediate IP ban on specific paths requested by non-authenticated users.

Security Level Characteristics – HTTP(S) Session Counter	User	Very Low	Low	Medium	High	Very High
Starting points	Any	0	0	0	0	0
Point limit	Any	2000	1500	1000	800	600
+ Points for each valid command	Any	0	0	0	0	0
+ Points for each invalid command	Any	300	300	300	300	300
+ Points for each request to non-public path	Anonymous	150	150	150	150	150
+ Points for each request to non-public path	Authenticated	0	0	0	0	0
+ Points for each request to non-public blacklisted path	Anonymous	2000	1500	1000	800	600
+ Points for each request to non-public blacklisted path	Authenticated	0	0	0	0	0
+ Points for each request to non-public whitelisted path	Any	0	0	0	0	0
- Points for each session clean exit	Authenticated	(All)	(All)	(All)	(All)	(All)
- Points at each timer tick (approximately every 10 seconds)	Any	(2000)	(750)	(350)	(300)	(150)
- Points at each timer tick if IP has been banned (exceeded limit)	Any	(200)	(75)	(35)	(30)	(15)

Customizations

Customized Scores

The default scores were created through careful analysis of typical client interactions under various DoS scenarios; however, your needs may require customization of the

default values, such as modifying only one parameter for a given sensitivity level to lower the chance of false positives under certain heavy but valid traffic patterns. To facilitate custom scenarios, EFT exposes all scoring values for each sensitivity in its Site configuration database. Please contact our support team for assistance in locating the appropriate table and applying new values.

Blacklist and Whitelist Overrides

To designate a blacklisted or whitelisted path for HTTP/S, set the following advanced properties:

> **NOTE:** Two advanced properties are available to either ignore or ban access to specific URLs:
> AutoBanAnonymousUnauthorizedAccessServicePathAllowList = Auto-ban will ignore processing non-public access to the specified paths.
> AutoBanAnonymousUnauthorizedAccessServicePathBlockList = Auto-ban will ban IP address access to the specified paths. (Not the full URL, just the service path.)

```
{
  "AutoBanAnonymousUnauthorizedAccessServicePathAllowList":[
       "/",
       "/custom-service",
       "/sp/samlv2/sso"
    ],
   "AutoBanAnonymousUnauthorizedAccessServicePathBlockList":[
       "/mysql-admin/index.php",
       "/administrator/phpMyAdmin/index.php",
       "/sql/sql-admin/index.php "
    ]
}
```

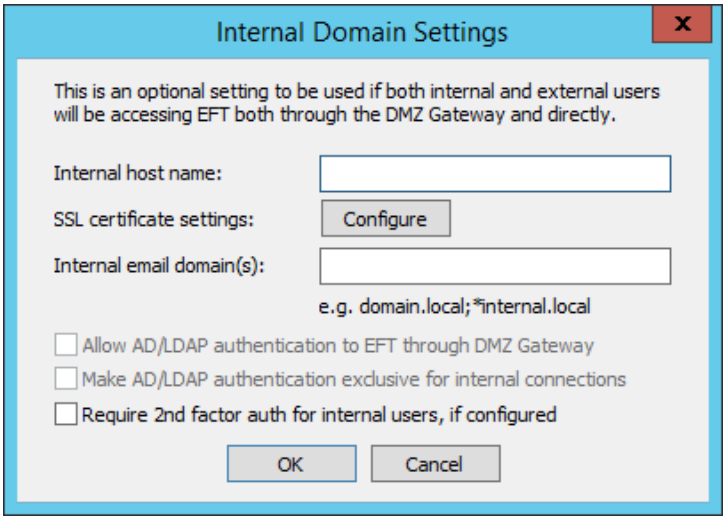
> **NOTE:** Refer to Advanced Properties for details of using advanced properties. s

Custom Scores for Admin Session

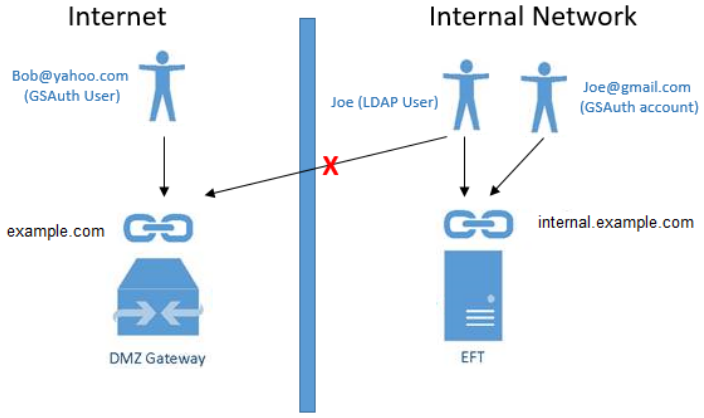
To designate a different sensitivity level for Administrative sessions, please use the advanced property: AutobanSensitivityLevelForAdminConnections

Internal Domain Settings

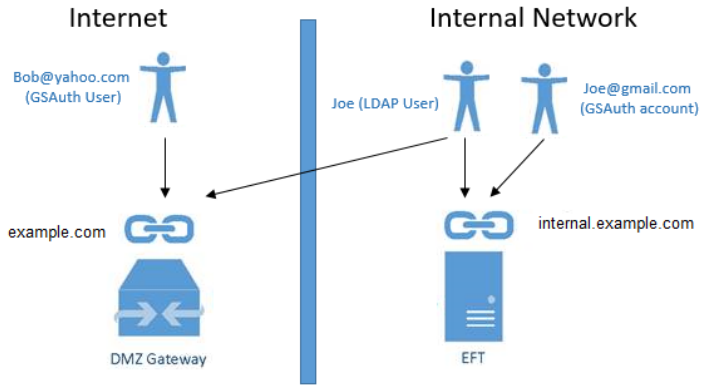
The **Internal Domain Settings**dialog box on the **DMZ Gateway**tab, is used to configure separate external and internal domain access. See Specifying External and Internal Domains and Allow LDAP Authentication through DMZ for more information about how to do that. Below are some diagrams to visually describe how the two check boxes, **Allow AD/LDAP authentication to EFT through DMZ Gateway** and **Make AD/LDAP authentication exclusive for internal connections**, interact to determine external and internal user access.



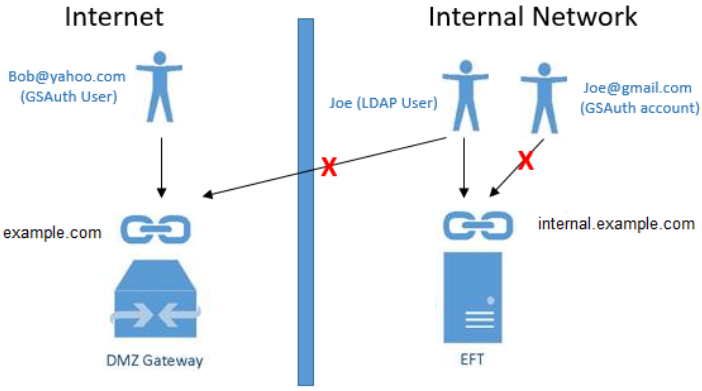
1. When neither box is selected, EFT and DMZ Gateway are in a "split domain" configuration:
    - AD and LDAP users are only allowed to log in through the internal (EFT) URL; they cannot use the external (DMZ Gateway) URL.
    - Globalscape authentication users can log in through the external (DMZ Gateway) URL or the internal (EFT) URL.



2. When the **Allow AD/LDAP authentication to EFT through DMZ Gateway** check box is selected, (but ***not*** the **Make AD/LDAP authentication exclusive for internal connections** check box):
    - Globalscape authentication users and LDAP users can log in using the internal (EFT) URL OR external (DMZ Gateway) URL. This configuration allows remote users to access EFT through DMZ Gateway.

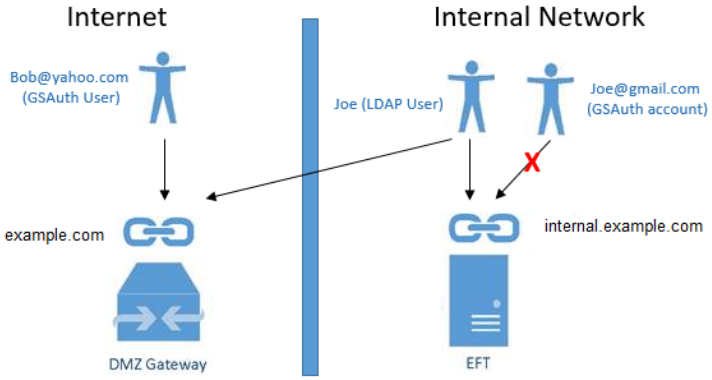


3. When the **Make AD/LDAP authentication exclusive for internal connections** check box is selected (but ***not*** the **Allow AD/LDAP authentication to EFT through DMZ Gateway** check box):
    - LDAP users can only log in using the internal (EFT) URL; they cannot use the external (DMZ Gateway) URL
    - Globalscape authentication users can log in using only the external (DMZ Gateway) URL; they cannot use the internal (EFT) URL



4. When both the **Allow AD/LDAP authentication to EFT through DMZ Gateway** check box and the **Make AD/LDAP authentication exclusive for internal connections** check box are selected:

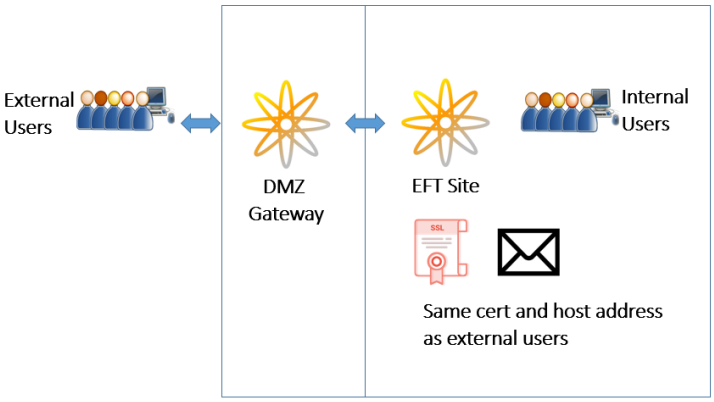
- Only AD or LDAP users can log in using the internal (EFT) or external (DMZ Gateway) URL
- Globalscape authentication users can only log in using the external (DMZ Gateway) URL; they cannot log in using the internal (EFT) URL.



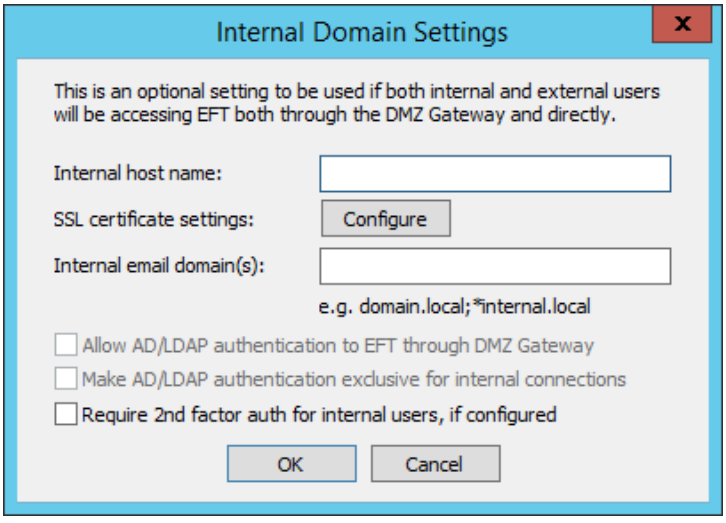
Specifying External and Internal Domains

(See also Allow LDAP Authentication through DMZ Gateway and Internal Domain Settings dialog box.)

By default, an EFT Site uses the same host address and SSL certificate, and email notifications create links to the same host address, as shown below.



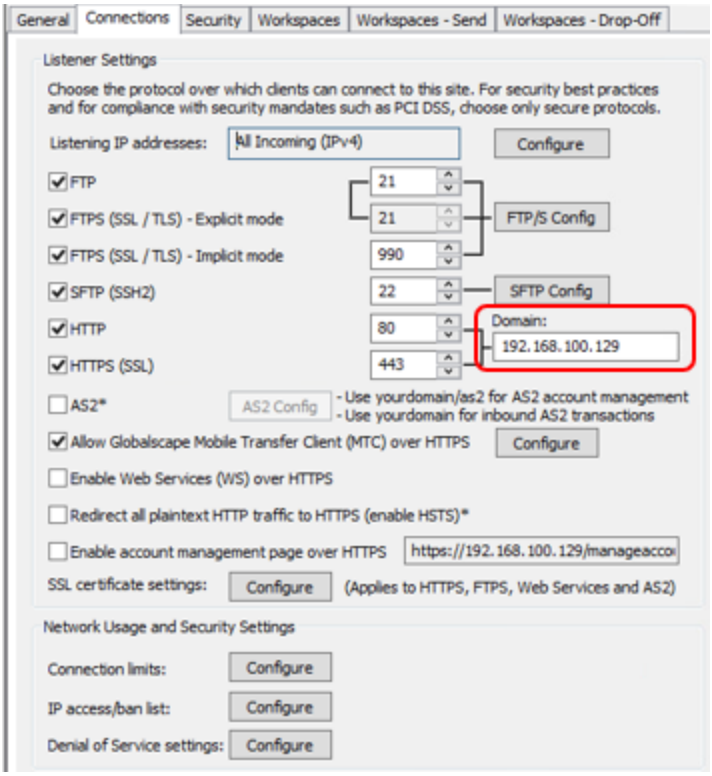
But suppose you want to create an environment in which users in their internal network can access EFT while at their internal workstation, but, for security reasons, you don't want those employees to connect to the server from outside the offices, such as when they are working at the local coffee shop or at a partner location. Also suppose that your company wants to segregate Workspaces participants that are external to the company network, such as vendors and customers.



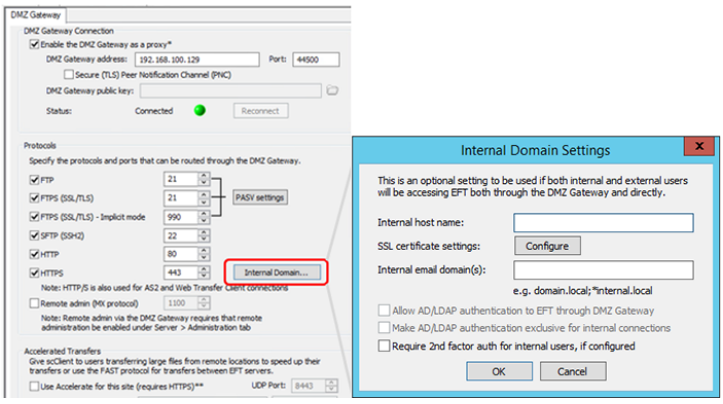
If you want EFT to distinguish INTERNAL access from EXTERNAL access, you can specify a host address for DMZ Gateway (Internet-facing) entry to EFT, and anything

flowing into EFT from that path will be considered external, then specify a different host address for internal users, as described below.

The *external domain* is specified on the Site's **Connections** tab:



An **Internal Domain** button is available next to the **HTTPS** port box on the **DMZ Gateway** tab of the EFT Site:



To specify the internal domain on a site

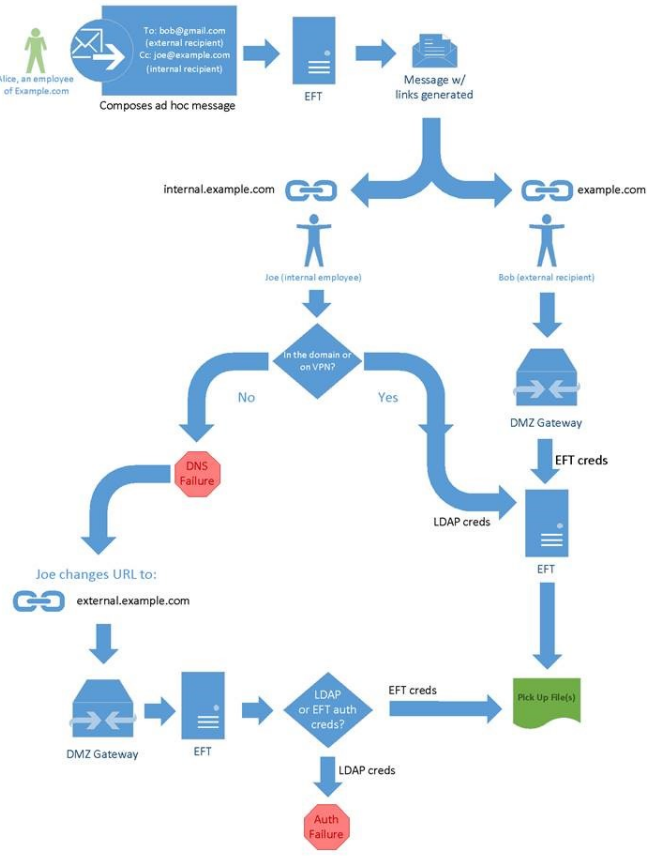
1. In the EFT administration interface, click the **Server**tab, then click the **Gateway** node.

2. On the **DMZ Gateway** tab, next to the **HTTPS** port box, click **Internal Domain**. The **Internal Domain Settings** dialog box appears.
3. In the **Internal host name**box, specify the URL through which internal users should log in to EFT. **Internal host name** is empty by default. Empty means that no domain matching is performed and notification links are not altered.
4. Click **Configure** to specify the SSL certificate. Internal users can use a different SSL certification than the external users. For example, for internal connections, and self-signed certificate created by EFT should be adequate.
5. In the **Internal email domains**box, specify one or more SMTP domains used by internal users, separated by semicolons. **Internal email domain**is empty by default. Empty means no email domain matching is performed and notification links are not altered.
6. Select the check boxes as needed:
    - **Allow LDAP authentication to EFT through DMZ Gateway** - Allows anyone connecting to EFT through DMZ Gateway to connect using LDAP authentication
    - **Make LDAP authentication exclusive for internal connections** - Prevents external connections to EFT through DMZ Gateway over LDAP
    - **Require 2nd factor auth for internal users** - Requires internal connections to EFT through DMZ Gateway to connect using LDAP authentication to use two-factor authentication, such as RSA SecurID
7. Click **OK**.

Workspaces Invitation and Notification Email Links

With separate internal and external domains defined, you can send different notification emails to internal and external accounts from the same EFT Site:

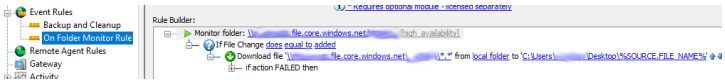
- If EFT sends an email where the email domain (after the "@" symbol) matches one of the specified "internal domains" values, any URLs formed by EFT and pointing to EFT in the email should be constructed using the internal host name (for example, internal.example.com).
- If EFT sends an email where the email domain (after the "@" symbol) does not match any of the specified "internal domains" values, any URLs formed by EFT and pointing to EFT in the email should be constructed using the default host name specified in the DMZ Gateway tab (for example, example.com).
- If no internal host name was specified, then EFT will use the default host name.


Alice, an employee of Example.com
To: bob@gmail.com (external recipient)
Cc: joe@example.com (internal recipient)
Composes ad hoc message
EFT
Message w/ links generated
internal.example.com
example.com
Joe (internal employee)
Bob (external recipient)
In the domain or on VPN?
No
Yes
DMZ Gateway
EFT creds
DNS Failure
LDAP creds
EFT
Joe changes URL to:
external.example.com
DMZ Gateway
EFT
LDAP or EFT auth creds?
EFT creds
Pick Up File(s)
LDAP creds
Auth Failure

Override VFS Credentials

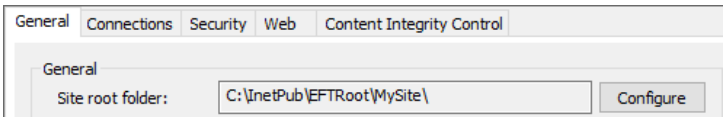
You can create a Virtual Folder that points to a file system share at a Azure Data Lake Storage URL, and provide your Azure Data Lake Storage credentials.

- **This topic assumes you've already created your Azure account.**Refer to https://azure.microsoft.com/en-us/services/storage/data-lake-storage/to read more about Azure Data Lake Storage.
- Containers created with Data Lake Gen 2 support can be monitored by an EFT Folder Monitor Event as long as the Azure container credentials and Active Directory domain trust relationship is enabled.

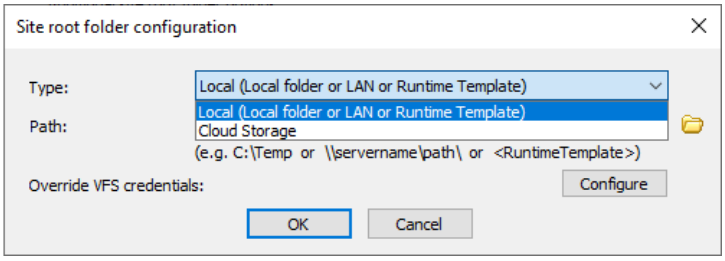


To enable the VFS credential override

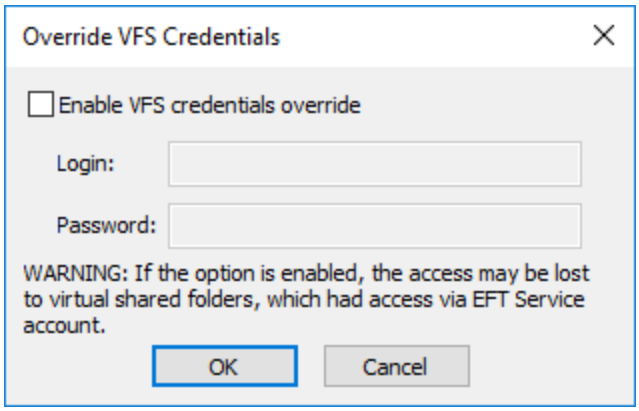
1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **General**tab.



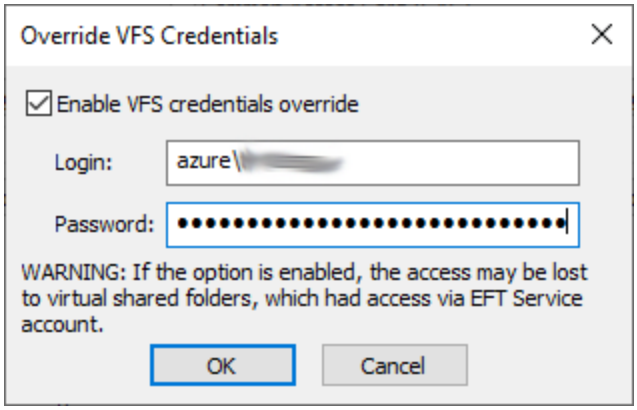
4. Next to the **Site root folder** box, click **Configure**. The **Site root folder configuration** dialog box appears.



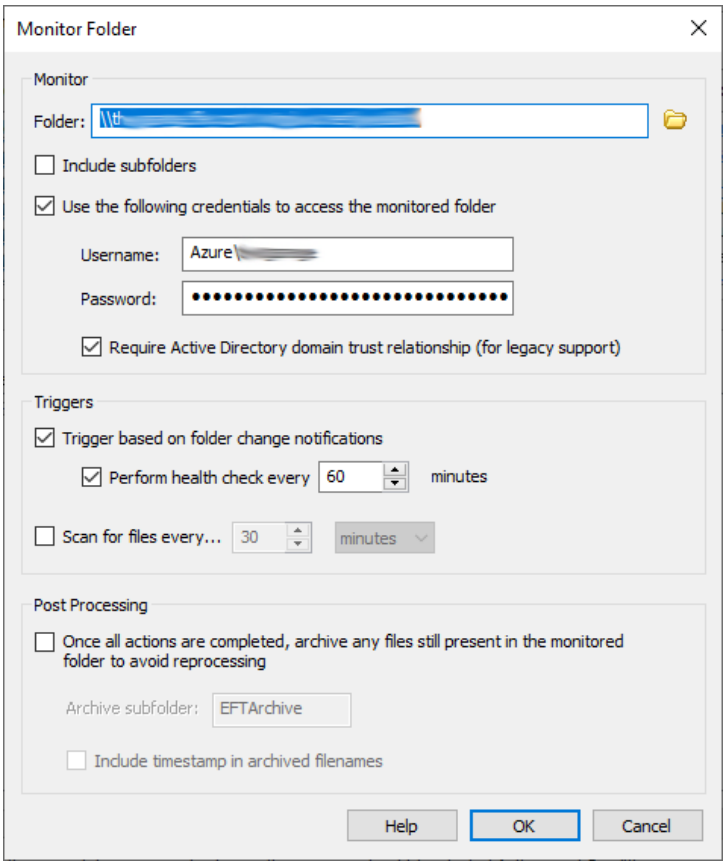
5. Click **Configure**. The **Override VFS Credentials** dialog box appears.



6. Select the **Enable VFS credentials override** check box. The **Login**and **Password** boxes become enabled.
7. Provide the credentials for your Azure Data-Lake supported container and the security key (password), then click **OK**.



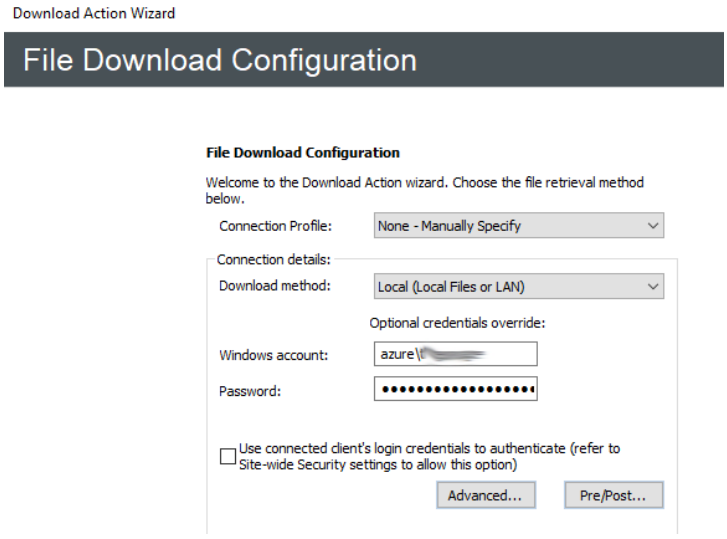
8. You can now create a Folder Monitor rule to monitor any changes made to that storage.

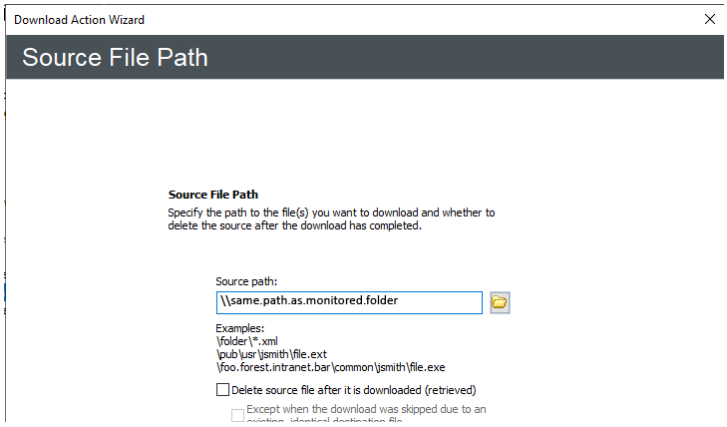


9. In the **Folder** box, provide the path to the Azure Data Lake Storage.
10. Select the **Use the following credentials** check box and provide your Azure Data Lake Storage credentials.
11. Select the **Require Active Directory domain trust relationship** check box.
12. Click **OK** to save the changes.
13. Add other Conditions or Actions as needed, then click **Apply** to save the Event Rule.

For Download Action:

In the File Download Configuration, use the credentials for your Azure Data-Lake supported container (from above) as the Windows account:


Download Action Wizard
File Download Configuration
File Download Configuration
Welcome to the Download Action wizard. Choose the file retrieval method below.
Connection Profile:
None - Manually Specify
Connection details:
Download method:
Local (Local Files or LAN)
Optional credentials override:
Windows account:
azure\
Password:
Use connected client's login credentials to authenticate (refer to Site-wide Security settings to allow this option)
Advanced...
Pre/Post...


Download Action Wizard
Source File Path
Source File Path
Specify the path to the file(s) you want to download and whether to delete the source after the download has completed.
Source path:
\\same.path.as.monitored.folder
Examples:
\folder*.xml
\pub\usr\jsmith\file.ext
\foo.forest.intranet.bar\common\jsmith\file.exe
Delete source file after it is downloaded (retrieved)
Except when the download was skipped due to an

Proxy Protocol

Instead of files waiting in a queue for a server to become available, load balancers for EFT HA Active-Active configuration are used to distribute traffic to available EFT servers. Adding a load balancer means that instead of EFT seeing the original client requests, it sees requests as though they had originated from the load balancer. In this case, EFT doesn't receive client information, such as IP address and port number, making it difficult to analyze traffic logs or other transfer details. Prior to EFT v8.0.5, when EFT is setup behind a load balancer, such as HAProxy or F5, when connections come in to EFT, the originating IP appears as that of proxy/LB, rather than origination client. (F5 has no native support for proxy protocol. You must create a custom i-Rule.)

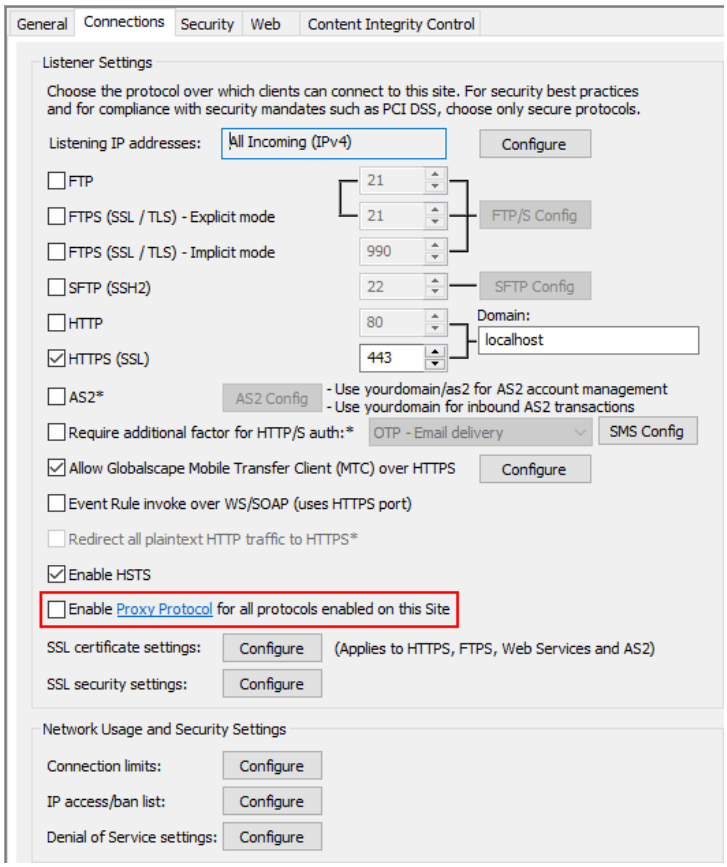
HAProxy developed a special "Proxy Protocol" to deal with this problem, which has since been adopted by load balancer manufacturers, proxies, and servers. Proxy Protocol provides a convenient way to safely transport connection information such as a client's address across multiple layers of NAT or TCP proxies. It is designed to require little changes to existing components and to limit the performance impact caused by the processing of the transported information.

Support was added in EFT v8.05 for Proxy Protocol version 1 to both our DMZ Gateway and to EFT. Proxy Protocol should only be used in conjunction with upstream load balancers or proxies that support and use proxy protocol; otherwise, EFT will abort inbound connections that lack the proper headers. There is no "mixed mode"; if Proxy Protocol is enabled, Proxy Protocol headers are required for that Site. If they aren't, connections are aborted. Also, Proxy Protocol is not supported for EFT as a client (that is, outbound transfers using Event Rules).

> **NOTE:** EFT and DMZ only support Proxy Protocol version 1. Proxy Protocol version 2 is not yet supported in EFT. Proxy Protocol version 1 uses a human-readable header format; version 2 uses a binary header format. EFT cannot read binary headers, so those connections would be aborted.

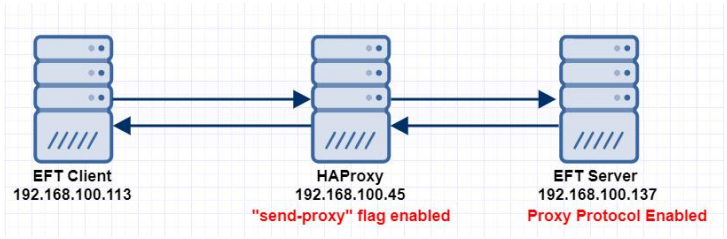
To enable Proxy Protocol

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site that you want to configure.
3. On the **Site > Connections** tab, select the **Enable Proxy Protocol for all protocols enabled on the Site** check box.
4. Click **Apply**to save changes.
5. Click the **Proxy Protocol**link to open https://www.haproxy.org/download/1.8/doc/proxy-protocol.txtto read more.

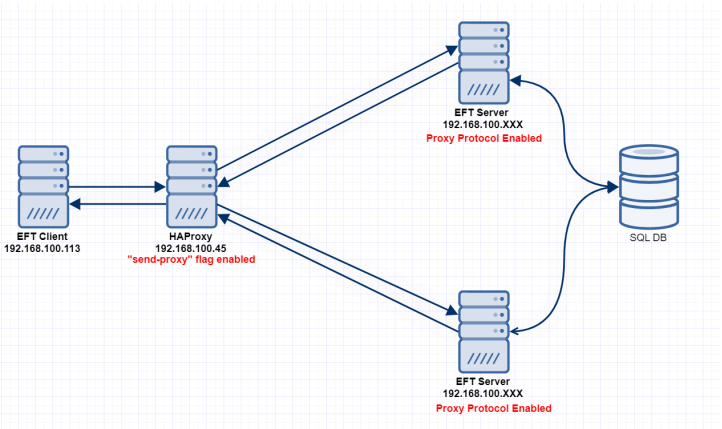


Information for HAProxy and other load balancers

Below is an illustration showing where the load balancer is placed in relation to the EFT client and server:



The Proxy Protocol is also supported in a cluster:



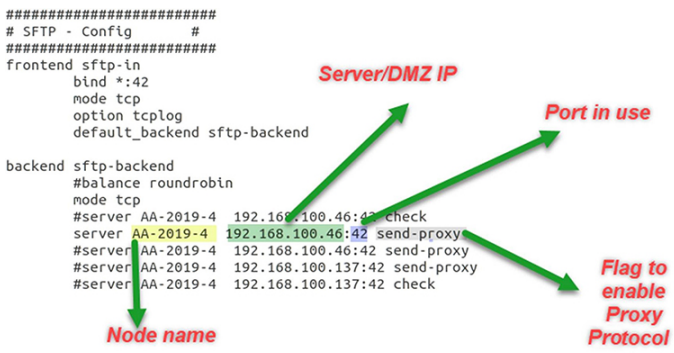
How to Modify the HAProxy Configuration File in Ubuntu

The **haproxy.cfg** configuration file (for the HAProxy load balancer) must be edited before using it. Each protocol has its own section in the file. Each protocol you will use must be edited for:

- Node or computer name
- EFT or DMZ Gateway IP address. You need to enter the EFT Site's IP address if you are not using a DMZ Gateway; otherwise, use the DMZ Gateway IP address.
- Port in use; specify the port set in EFT or DMZ Gateway

To change the configuration

1. Add or remove the # to enable or disable the proxy flag.



2. Make the changes to the configuration file using the IP address of your EFT Sites or DMZ Gateway.
3. Update the relevant sections for each protocol (HTTP/S, FTP/S, SFTP).
4. Enable the proxy protocol by setting the "send-proxy" flag.
5. Save the changes, then, restart the HAProxy Service (service name = haproxy)

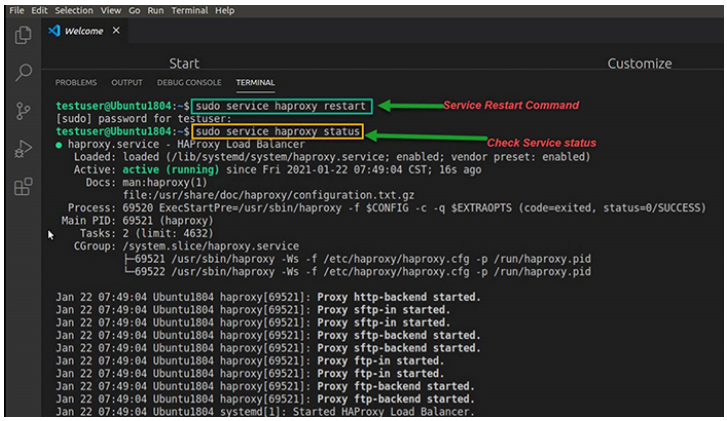
In Ubuntu/Linux:

- Command to start the service:

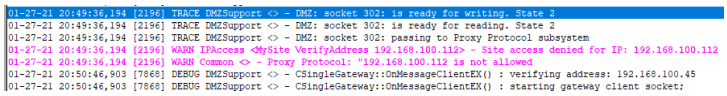
```
sudo service haproxy restart
```

- Command to check the status of the service:

```
sudo service haproxy status
```



This is an example of what the log captures:



For other load balancers

- For the Barracuda load balancer Proxy Protocol configuration, refer to their documentation at https://campus.barracuda.com/product/webapplicationfirewall/doc/79465780/how-to-enable-proxy-protocol/.
- The F5 BIG-IP does not have native support for Proxy Protocol, but you can configure it using iRules. Refer to their documentation for details: Article: K40512493 - Proxy protocol for the BIG-IP (f5.com).
- For Digital Ocean load balancers Proxy Protocol information: DigitalOcean Blog | DigitalOcean Load Balancers Now Support Proxy Protocol.

Renaming a Site

You can rename a Site by editing it (as administrator) in SQLite when the EFT server service is stopped.

To rename the Site

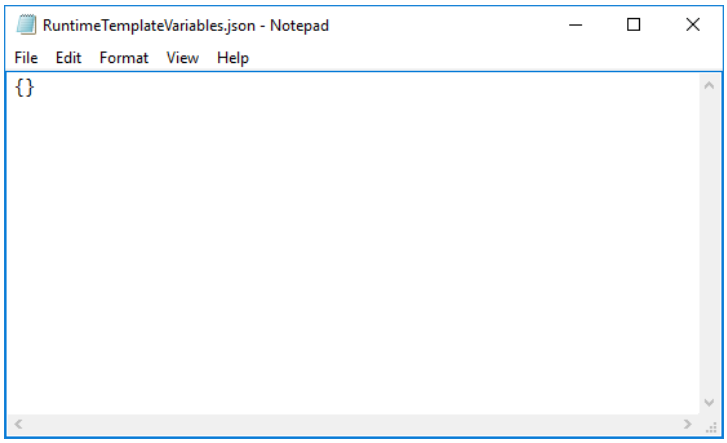
1. Log out of the administration interface.
2. Stop the EFT server service.
3. Open the SiteConfig<GUID>.db file in the SQLite DB Browser. (https://sqlitebrowser.org/)
4. On the **Browse Data** tab, open the Site table.
5. Edit the Site **Name**.
6. Start the EFT server service.
7. Log in to the EFT administration interface.

Runtime Template Variables

Runtime template variables are used to replace reference values at runtime.

A JSON file named **RuntimeTemplateVariables.json** (default: C:\ProgramData\Globalscape\EFT Server\RuntimeTemplateVariables.json) is used to store the variable and its assigned value and is read by EFT when the server service is started. In a clustered environment, the JSON can be stored on the shared drive.

The **RuntimeTemplateVariables.json**file is in the format of a normal JSON file, with "name": "value". Just like the AdvancedProperties,json file, the file is empty. Only the non-default settings that you add will appear in the file. For HA installations, the file is saved in the HA shared configuration location.



All non-password fields that accept non-validated, user-input string values accept template variables in addition to context variables and normal strings. For all secret/password fields that are masked (for example, SAS token, S3 secret key, copy/move password), if the value entered starts with a left bracket < and ends with a right bracket >, then it will be interpreted as a template variable.

Runtime variables can be used to store not only the path for site config or login for download action, it can also be used for message templates for things like email notifications.

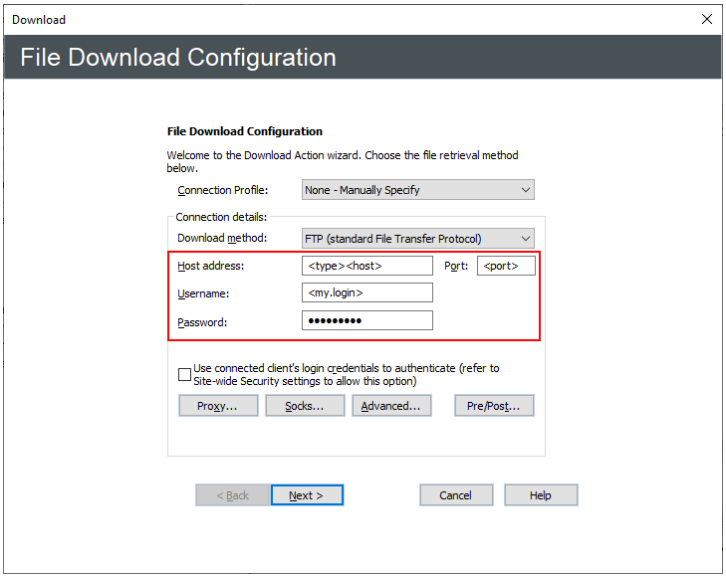
Symbols (such as the Euro symbol) are not allowed in the JSON file. EFT will read everything up to the symbol and then stop readying the JSON; the site will not start due to unallowed characters.

To use runtime template Variables

Add variables to the **RuntimeTemplateVariables.json** file:

```
{
"site_path":"C:\\InetPub\\EFTRoot\\MySite\\",
"my.login":"user1",
"type":"local",
"host":"host",
"port":"21"
}
```

File download action setup wizard then uses the variables in the applicable fields:



Action fields above would be evaluated as indicated in the **RuntimeTemplateVariables.json** file:

- Host address: "localhost"
- Username: "user1"
- Port: 21

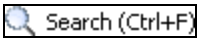
Searching a Site

You can use EFT's search feature to find and open an item on a Site, such as a user account, a workflow, or Event Rule. The table below indicates which objects are searched and which details within the objects can be found.

Object Type	Name Search	Details Search
Settings Template	name	name
User	name	name, account details (e.g. email address), home folder
Group	name	name
Command	name	name, description, path, parameters
Advanced Workflows	name	name, description
Event Rule	name	name, paths, download/offload usernames and host names, Send email Action email addresses and names
Connection Profiles	name	name, description, connection details

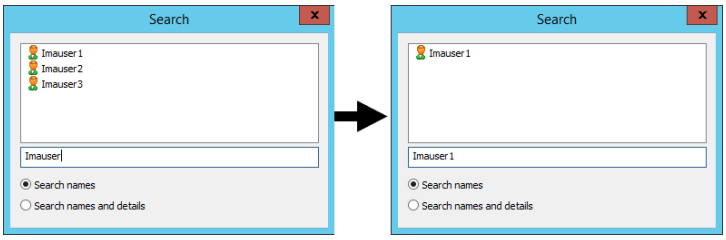
For example, you can search for an email address, and not only find the user to whom the email address belongs, but also any Event Rules that reference that email address.

To find an object on a Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Site** that you want to search.
3. Press CTRL+F or click the **Search**node 

in the Site tree.
   The **Search** dialog box appears.

4. At the bottom of the **Search**box, click **Search names** to find only the names of objects or click **Search names and details** to search within objects for things like email addresses or paths. (Refer to table above to see which objects contain searchable details.)
5. In the text box at the bottom, type the text to find. EFT will automatically search as you type and display the results in the top box. You can scan through the list to find the one you want, or you can keep typing until the object you are looking for appears.

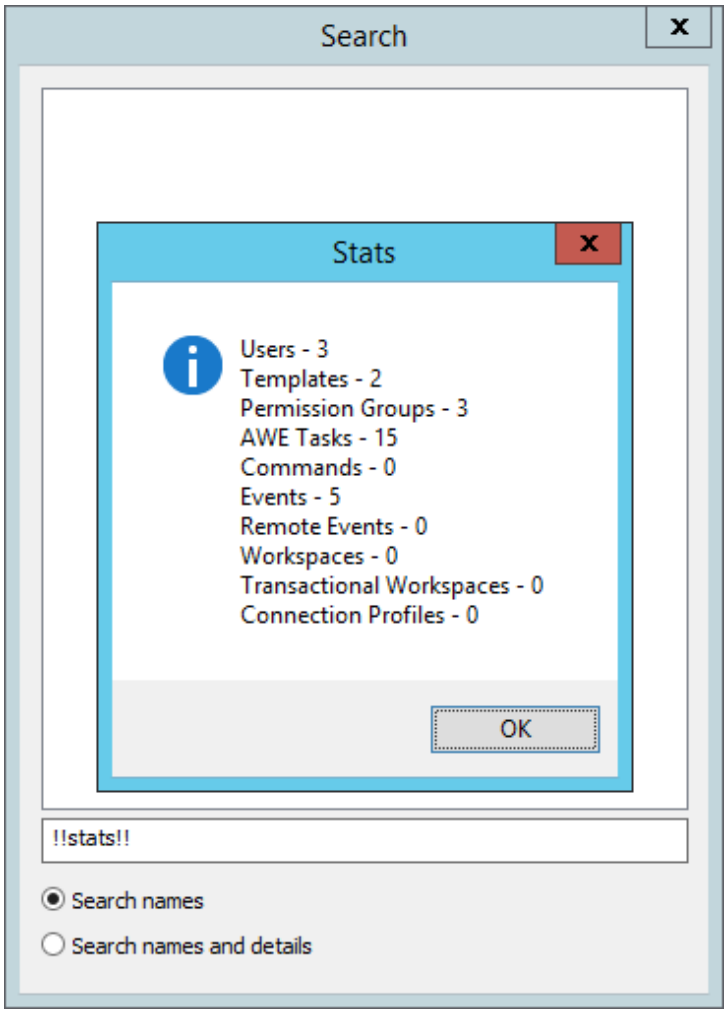


If you enter a character that is not found in any strings, the "<<NO MATCHES FOUND!>>" message appears.

6. Click an item in the tree to open the item and close the **Search** dialog box. For example, if you click a username, that user's **General**tab appears.
    - You can click the **Search**node again to reopen the **Search**dialog box with the latest search results displayed. Also, the latest search results are updated as you create new items. For example, suppose you have a user1, user2, and user3 and you searched for "user." The **Search**dialog box will show user1, user2, and user3, and any Group, Command, Event Rule, or Workflow on that Site that contains the word "user." If you click a search result, close the **Search**dialog box, and then create user4, the next time you open the **Search** dialog box, user4 will now appear in the search results (until you clear "user" from the search field).
7. To get a list of each item and the number of items, type:

    `!!stats!!`

    A message box appears similar to this one:



    - Click **OK** to close the message.
8. Click the **X**in the upper right corner to close the **Search**dialog box.

Setting Maximum Concurrent Socket Connections

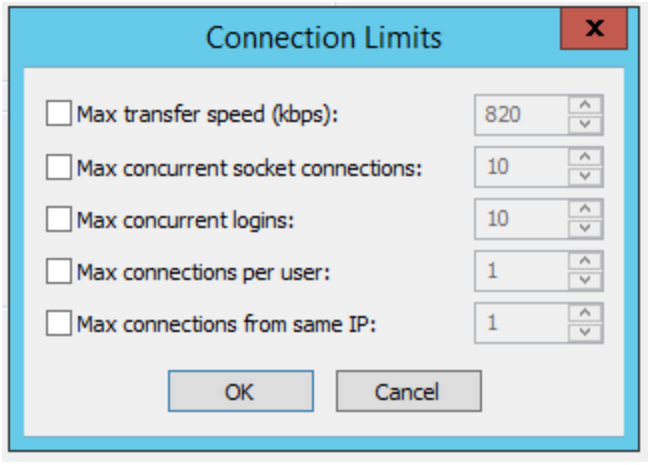
The **Max concurrent socket connections** check box limits the amount of socket or low-level connections on a Site allowed by EFT. When this limit is reached, any subsequent connection attempt generates a socket or network error in the client. It reacts as if EFT is not available, because EFT refuses the connection entirely.

If EFT is configured as an anonymous FTP server, you should limit connections per user. In this case, EFT will allow the user to partially connect before being told that EFT is full or busy, which is a more graceful way of denying the connection.

Maximum number of socket connections to EFT is configured on a Site. If you have multiple Sites, you can configure some Sites to allow more users than other Sites.

To restrict the number of socket connections

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site that you want to configure.
3. In the right pane, click the **Connections** tab.
4. Next to **Connection limits**, click **Configure**. The **Connection Limits** dialog box appears.



5. Select the **Max concurrent socket connections** check box, then specify the maximum number of users you want to allow at any given time. If the box is cleared, EFT does not restrict the number of users.
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

Related Topics

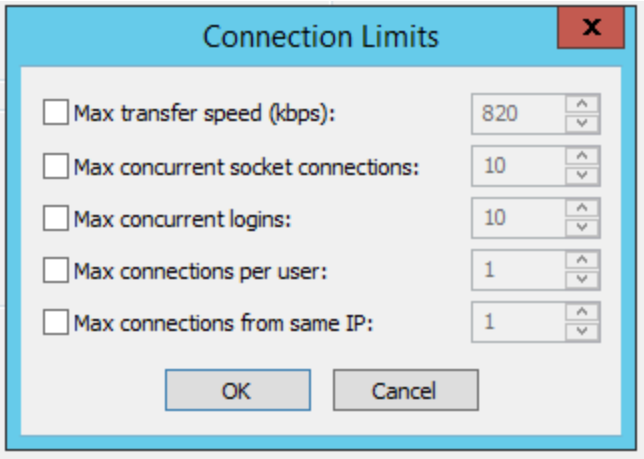
- Setting Maximum Transfer Speeds
- Setting Maximum Concurrent Logins
- Setting Maximum Connections for Users
- Setting Maximum Connections per IP

Setting Maximum Concurrent Logins

You set the maximum number of logins to EFT on the Site. If you have multiple Sites, you can configure some Sites to allow more connections than other Sites.

To restrict the number of socket connections

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site that you want to configure.
3. In the right pane, click the **Connections** tab.
4. Next to **Connection limits**, click **Configure**. The **Connection Limits** dialog box appears.



5. Select the **Max concurrent logins** check box, then specify the maximum number of logins you want to allow at any given time. If the box is cleared, EFT does not restrict the number of logins.
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

Related Topics

- Setting Maximum Transfer Speeds
- Setting Maximum Concurrent Socket Connections
- Setting Maximum Connections
- Setting Maximum Connections per IP

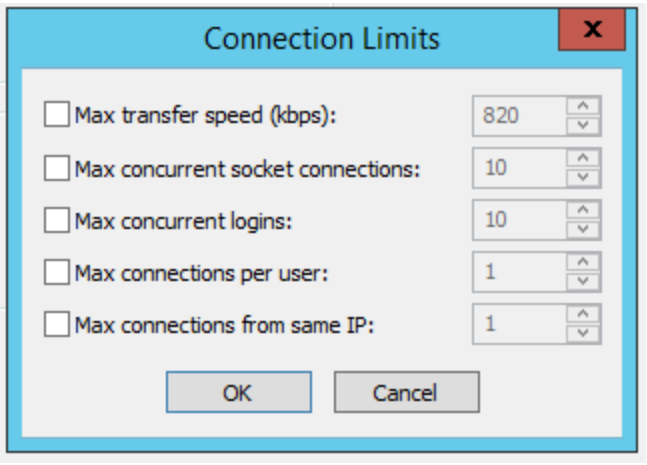
Setting Maximum Connections per User

You can set the maximum number of simultaneous connections for a user on the Site, Settings Template, and/or for each user.

The Site sets the limit for all sub levels. For example, if the Site's **Max connections per user** is 5, and a user's **Max connections per user** is set to 10, the user can still only connect to the Server 5 times simultaneously.

To set maximum connections per user

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site, Settings Template, or user that you want to configure.
3. In the right pane, click the **Connections**tab.
4. Next to **Connection limits**, click **Configure**. The **Connection Limits** dialog box appears.



5. Select the **Max connections per user** check box, then type or use the arrows to select a number. (You must specify an integer between 1 and 99999.)
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

Related Topics

- Setting Maximum Transfer Speeds
- Disconnecting Users on Timeout
- Setting Maximum Concurrent Logins
- Setting Maximum Connections per IP

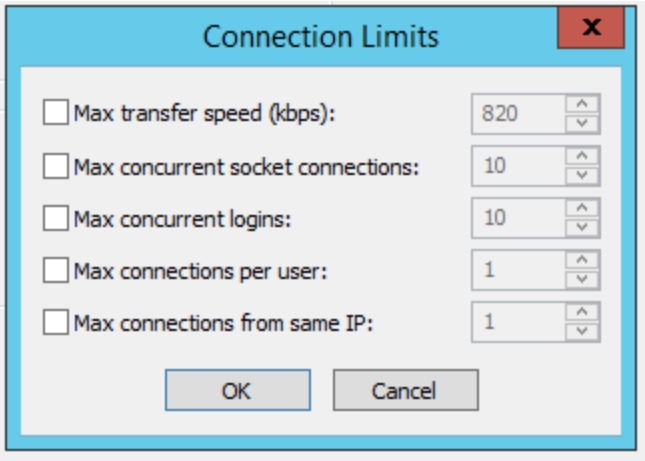
Setting Maximum Connections per IP Address

You can set the maximum number of simultaneous connections emanating from the same IP address on the Site, Settings Template, and/or for each user.

The Site sets the limits of the user accounts and the Settings Templates. That is, you cannot specify a larger number on the Settings Template or user account than is set on the Site.

To set maximum connections per IP address for a Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site, Settings Template, or user account that you want to configure.
3. In the right pane, click the **Connections** tab.
4. Next to **Connection limits**, click **Configure**. The **Connection Limits** dialog box appears.



5. Select the **Max connections from same IP** check box and type the maximum number of simultaneous connections you want to allow from the same IP address. (You must specify an integer between 1 and 99999.)
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

Related Topics

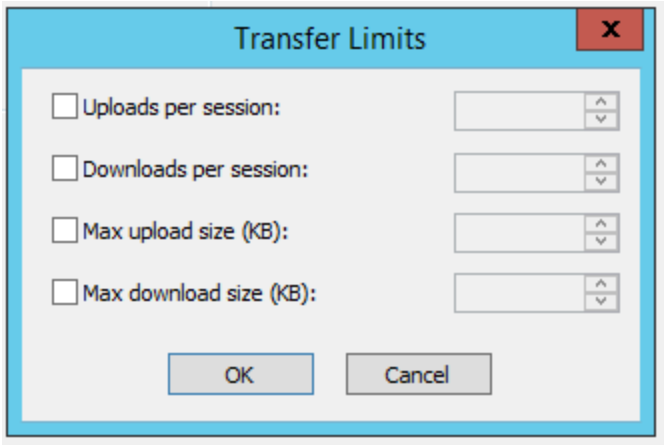
- Setting Maximum Transfer Speeds for a Site
- Setting Maximum Concurrent Socket Connections to a Site
- Setting Maximum Concurrent Logins to a Site
- Setting Maximum Connections for Users on a Site

Setting Maximum Transfers per Session

You can set a limit on the number of file transfers allowed per login session for the Settings Template or per user.

To set the maximum allowed transfers per session

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Settings Template or user account that you want to configure.
3. In the right pane, click the **Connections**tab.
4. Next to **Transfer limits**, click **Configure**. The **Transfer Limits** dialog box appears.



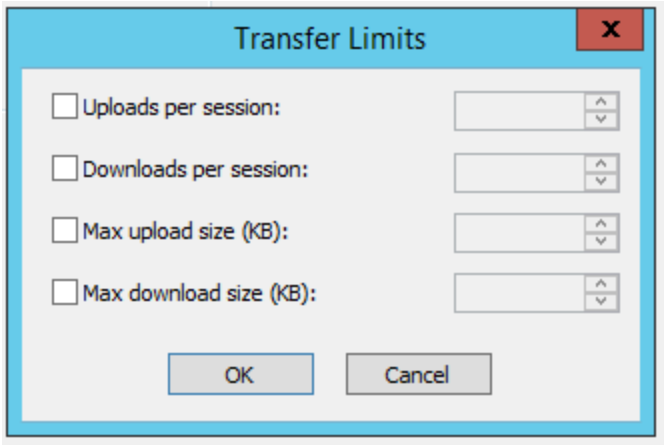
5. Select the **Uploads**and/or **Downloads per session** check box and specify the maximum number of uploads/downloads the user may transfer during a session.
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

Setting Maximum Transfer Size

The *maximum transfer size* limits the user to a specified number of upload or download kilobytes per session. FTP does not send information to EFT regarding the number of bytes that a user sends. A user can start a transfer of virtually any size; however, once the limit is reached, EFT will not transfer the rest of the file.

To set the maximum transfer size

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Settings Template or user that you want to configure.
3. In the right pane, click the **Connections**tab.
4. Next to **Transfer limits**, click **Configure**. The **Transfer Limits** dialog box appears.



5. Select the **Max Upload/Download Size** check boxes and specify the maximum amount of data (in kilobytes) the user may transfer during a session.
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

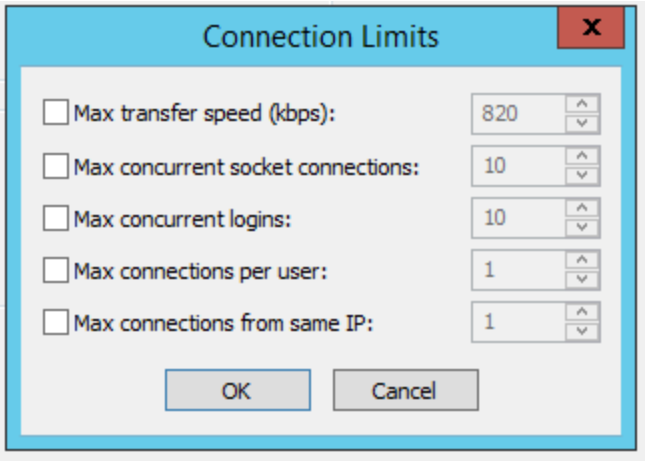
Setting Maximum Transfer Speeds

You can control a user's maximum transfer speeds at the Site level, Settings Template, and/or for each user.

The Site sets the limits of the users and Settings Templates. That is, you cannot set the maximum transfer speed on the Settings Template or for user accounts higher than it is set on the Site.

To configure maximum transfer speeds on the Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site, Settings Template, or user that you want to configure.
3. In the right pane, click the **Connections** tab.
4. Next to **Connection limits**, click **Configure**. The **Connection Limits** dialog box appears.



5. Select the **Max transfer speed (kbps)** check box, then specify the maximum transfer speed for the Site. If the check box is cleared on the Site, the maximum transfer speed is not specified for the Site, but can be specified in the Settings Template or for each user account.
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

Related Topics

- Setting Maximum Concurrent Socket Connections to a Site
- Setting Maximum Concurrent Logins to a Site

- Setting Maximum Connections for Users on the Site
- Setting Maximum Connections per IP for a Site

Specifying File Deletion Options

The Regulatory Compliance Module (RCM) provides a data sanitization/data wiping option, which satisfies PCI DSS requirements. If you do not activate the module, this feature is disabled after the trial expires.

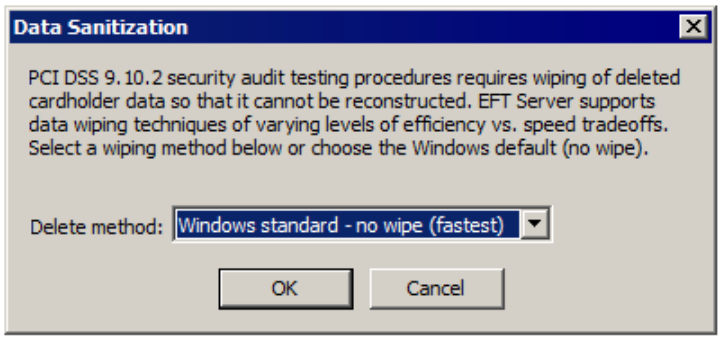
You can configure EFT to securely delete or purge a file by writing over the initial data using encrypted and/or pseudorandom data. A menu of purging methods is available; available options depend on the library used.

- The 3-pass DoD method overwrites all addressable locations with a character and its complement, then a random character, and does this three times.
- The pseudorandom data wiping method does the following:
    1. Initializes the wincrypt library
    2. Fills the file with randomly generated data from the wincrypt library
    3. Flushes the data to disk
    4. Deletes the file from file system calling the standard function DeleteFile()

*.pgp files are automatically excluded from the wipe process. When wipe is enabled, ANY delete operation also includes the wipe (sanitization) process.

To specify a delete method

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site that you want to configure.
3. In the right pane, click the **Security**tab.
4. In the **Data Security** area, next to **Secure data removal**, click **Configure**. The **Data Sanitation** dialog box appears.



5. In the **Delete method**box, click the list to specify one of the following methods:

- Windows standard (fastest)
- Pseudorandom data (medium)
- 3-pass DoD 5220.22-m (slow)

6. Click **OK** to close the dialog box.
7. Click **Apply**to save the changes on EFT.
8. A message appears when the purging mechanism is changed to anything other than the Windows standard delete method.

For further reference regarding data wiping, see the following articles:

(These links are outside of Globalscape's domain and could change.)

- *Data remanence*:http://en.wikipedia.org/wiki/Data_remanence, specifically the section titled "Standard Patterns for Purging": http://en.wikipedia.org/wiki/Data_remanence#Standard_patterns_for_purging
- US DoD 5220.22-M Standard, defined in the US National Industrial Security Program Operating Manual of the US Department of Defense: http://en.wikipedia.org/wiki/National_Industrial_Security_Program
- "Secure Deletion of Data from Magnetic and Solid-State Memory": http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/

Unicode Exceptions

Most of the EFT interface supports Unicode characters. (Refer to Unicode File Transfers for details. The table below lists exceptions to Unicode support in EFT.

Area	Storage (Internal Representation on Disk)	GUI (Allowed and Displayed)	Usage	Remarks
General				
All domain (host) fields	Unicode	Unicode	7-bit ASCII	IDN (Internationalization of Domain Names) support by converting Unicode to Punycode upon use. From a user (presentation) perspective and EFT's internal representation, it will be Unicode.
All email address fields	Unicode	7-bit ASCII	7-bit ASCII	Conversion to Unicode for storage, but downgrade on usage. No risk/potential for loss of fidelity, as all chars limited to <128 ASCII. You can paste in Punycode ASCII characters directly for the domain portion if you must have Unicode domains for email addresses.
SMTP settings (username + password)	Unicode	7-bit ASCII	7-bit ASCII	Conversion to Unicode for storage, but downgrade on usage. No risk/potential for loss of fidelity, as all chars limited in GUI/usage to <128 ASCII.
Installer	8-bit ASCII	8-bit ASCII	8-bit ASCII	See Installer – ASCII ONLY below for potential problems
Keys and OpenPGP				
SSL CN field	8-bit ASCII	8-bit ASCII	8-bit ASCII	RFC allows for Unicode but OpenSSL handles the value as ASCII
SSL priv. key pass	8-bit ASCII	8-bit ASCII	8-bit ASCII	Passwords stored as octets sequence using same encoding as UI (ASCII)
SSH priv. key pass	8-bit ASCII	8-bit ASCII	8-bit ASCII	Passwords stored as octets sequence using same encoding as UI (ASCII)
OpenPGP priv. key pass	8-bit ASCII	8-bit ASCII	8-bit ASCII	Veridis limitation. Passwords stored as octets sequence, 8-bit ASCII.

Area	Storage (Internal Representation on Disk)	GUI (Allowed and Displayed)	Usage	Remarks
OpenPGP filename and pathnames	n/a	n/a	8-bit ASCII	Unicode filenames will be supported, but the will be temporarily converted to ASCII.
OpenPGP key name	8-bit ASCII	8-bit ASCII	8-bit ASCII	OpenPGP module does not support Unicode
OpenPGP public and private keyring paths	8-bit ASCII	8-bit ASCII	8-bit ASCII	OpenPGP module does not support Unicode
RSA				
RSA Conf.reg path	8-bit ASCII	8-bit ASCII	8-bit ASCII	RSA dll only takes ASCII path values
RSA usernames and passwords	Unicode	Unicode	8-bit ASCII	RSA does not support Unicode. We will downgrade to ASCII on usage. Potential loss of fidelity resulting in failed authentication attempts.
ARM				
ARM report content	Unicode (audited)	8-bit ASCII (reported)	8-bit ASCII (reported)	Loss of fidelity for UTF-8 chars that don't match local code page for ext. ASCII. The VSReport Designer does not support Unicode.
AS2				
AS2 outbound	n/a	n/a	8-bit ASCII	AS2 does not support Unicode encoded filenames. We can't downgrade to ASCII as we would be violating Drummond, thus we will simply disallow and log error.

Area	Storage (Internal Representation on Disk)	GUI (Allowed and Displayed)	Usage	Remarks
AS2 inbound	n/a	n/a	8-bit ASCII	AS2 does not support Unicode encoded filenames. Unlike offloads, EFT inbound can't detect whether the incoming file is Unicode encoded or not, thus we will always hand the file off to the AS2 component, with potential for mixed results. The outcome will be: a) an ASCII encoded filename, b) a failed transaction, or c) an ASCII encoded unique filename. Reference the AS2 Inbound Operations Use Case Cheat Sheet for additional guidance.
RADIUS				
RADIUS NAS ID	Unicode	8-bit ASCII	8-bit ASCII	EFT 6.4 used 8-bit ASCII. EFT 6.5 will represent as UNICODE strings (internally) and then downgrade to 8-bit ASCII on use. Also limited to ASCII in UI.
RADIUS special cases				
RADIUS shared secret	Unicode	Unicode	UTF-8	RFC says nothing about RADIUS password. EFT 6.4 used 8-bit ASCII. EFT 6.5 uses UTF-8. This difference (between earlier versions of EFT and version 6.5 and the resulting potential loss of fidelity is why this item is included on this list (even though it is UTF-8)
RADIUS usernames	Unicode	Unicode	UTF-8	RADIUS usernames and the shared secret can be UTF-8 strings.
HTTP				
EFT client action HTTP/S credentials	Unicode	n/a	Base64 encoding of UTF-8 string	
EFT client action HTTP/S Proxy	Unicode	n/a	Base64 encoding of UTF-8 string	

AS2 Inbound Operations

AS2 client compliance with RFC 2184	File encoding of source file on disk	Resulting change to file encoding in transit	EFT treatment (resulting encoding and/or loss of fidelity)
Standard AS2 client. Does not comply with RFC 2184. It relies on filename=<text encoded in ASCII> NOTE: Majority of known AS2 clients	ASCII	ASCII (no change)	Filename integrity maintained. No loss of encoding fidelity. Normal use case. This is essentially 7 and 8-bit ASCII transfers when working with standard ASCII only AS2 clients works perfect.
	Unicode	ASCII – down converts to "??????" or nonsense characters.	/n component will fail to process because "????" is an invalid filename. The transfer will result in a failure to write to disk. EFT must log this as an error in eft.log.
AS2 client is compliant with RFC2184. That is, uses filename*= utf-8''<text encoded in UTF-8>	ASCII	ASCII (no change)	Filename integrity is NOT maintained. /n component will process but will convert the filename to a unique 8-bit ASCII filename. However, there won't be a loss of encoding fidelity. EFT will log as warning that filename was changed.
	Unicode	Unicode (no change)	Filename integrity is NOT maintained. /n component will process but will convert the filename to a unique 8-bit ASCII filename; There is also a loss of encoding fidelity as it is down converted to ASCII. EFT will log as warning that filename was changed.
AS2 Other/Miscellaneous Limitations			
AS2 ID (identifier)	ASCII only	ASCII only	EFT displays a message indicating that Unicode is not allowed.

Q: Why is there no AS2 outbound cheat sheet?

A: EFT controls outbound and disallows UTF-8 encoded filenames from being transferred (see main exceptions above). EFT is more lenient on the inbound side, depending on the use cases described above.

PGP SDA Exceptions

If source filename is:	If source path is:	Resulting SDA name:	If extract path is:	Result
Unicode	n/a	n/a	n/a	Will fail to generate SDA
ASCII	Unicode	ASCII	ASCII	Works perfect. Everything preserved
	ASCII			
ASCII	Unicode	ASCII	Unicode	Will fail to extract
	ASCII			

Installer – ASCII ONLY

EFT's installer is not Unicode compliant. You cannot define Unicode values in the installer for app data path, administrator name, etc. The values can be changed in EFT, but with serious ramifications.

Unicode File Transfers

EFT's support for UTF-8 encoded Unicode characters extends to:

Inbound protocols:

- HTTP/S
- SFTP

Event Rules:

- Copy/Move and Download action wizards (all protocols) when specifying "UTF-8" as the filename encoding, and when using wildcards for the source filename, e.g. (*.dat, or *.*)
- Advanced Workflow Engine when passed filename-related context variables (for example, %FS.PATH%, %FS.FILE_NAME%, etc.)

Auditing:

- EFT's summary Client Log (CL)
- EFT's extended client logs (e.g. LAN copy, FTP extended, and SFTP debug logs)
- EFT's debug log (Log4Cplus)

Exclusions*:

- FTP protocol (inbound)
- All Event Rule actions that process a filename related context variables (e.g. %FS.PATH%, %FS.FILE_NAME%, etc.); the only exception is Advanced Workflow module (AWM) actions
- Folder Monitor events. Windows will notify EFT when a Unicode file is dropped into a monitored folder, but EFT cannot (at present) pass the UTF-8 encoded filename context variable off to Event Rule actions for processing.

  The only exception being when the action is an AWM action, in which case UTF-8 encoding is preserved. Do not be tempted to use wildcards as the source filename for Folder Monitor rules (even if pollingonly is used), as this will lead to race conditions and other problems. Wildcards should only be used in rules that don't use filename context variables, such as Timer, user, or system related events.
- ARM database and all logs not explicitly mentioned above
- No User Interface (UI) components. This means you cannot specify Unicode characters in Event Rules or anywhere else in the administration interface
- No COM API support for Unicode
- EFT does not support UTF-8 filenames over AS2

*UTF-8 will be more comprehensive in a future version. Refer to Unicode Exceptions for more information.

Unicode FAQs

The FAQs below are provided to answer questions you may have regarding EFT's Unicode support.

Q. What is Unicode?

A. Unicode is a standard that provides a unique number for every character, regardless of platform, program, or language. Systems that don't support Unicode and without the proper ANSI code page will render characters such as 大きい魚 ???????. or .

Q. Does EFT support Unicode?

A. EFT partially supports Unicode and is moving towards full support.

Q. What about UTF-8?

A. UTF-8 is simply a popular mechanism for encoding Unicode characters using one or more bytes. Prior to supporting UTF-8, EFT used ANSI code pages to view filenames in the intended format (on the target system when browsing with the WTC or PTC).

Q. What other mechanisms for encoding Unicode characters does EFT support?

A. EFT uses full double byte UCS-2 encoding at the file system (I/O) level, UTF-8 encoding within EFT, and ASCII everywhere Unicode is not yet supported.

Q. Does EFT support UTF-8 for file transfers?

A. EFT preserves UTF-8 encoded filenames when transferring files over HTTP and SFTP when acting as a server, and over all supported protocols when acting as a client, when certain conditions are met (see next question).

Q. What about EFT's Event Rules?

A. EFT's Copy/Move and Download Action wizards (across all protocols) support Unicode when you specify "UTF-8" as the filename encoding method (radio button in the wizard), and when using wildcards for the source filename, e.g. (*.dat, or *.*). However, UTF-8 is not supported for these Actions if you use %FS.PATH% or any other variable for the source filename, which means the Folder Monitor Event cannot be used to offload files and conserve their Unicode format. In fact, the only Action that supports UTF-8-encoded filenames through context variables is an AWM workflow task.

Q. Which client applications can I use to see Unicode filenames when I transfer files to EFT?

A. EFT's Web Transfer Client (WTC) supports UTF-8. For file transfer applications that do NOT support UTF-8, Unicode filenames will appear as "???????.exe" when using them to transfer files to/from EFT. CuteFTP v9 supports UTF-8.

Q. Can EFT audit or log filenames or other data with Unicode characters?

A. EFT's summary Client Log (CL), extended client logs (LAN transfer logs, FTP logs, SFTP debug logs), and debug log (eft.log), and AWM logs all support Unicode characters. EFT's EX logs, cmd out logs, and ARM (both auditing and reporting) do NOT support Unicode characters.

Q. If this filename: 梅雨右折車線_XYZ.ISO is transferred to EFT, how will it appear on disk? In reports? In EFT's Event Rules?

A. EFT will store the file to disk and conserve the original Unicode filename. The filename will be audited properly to EFT's eft.log, but will be down converted to ASCII when audited to the EX log and to the ARM database, resulting in a filename that may look like this: ??????_XYZ.iso, which is also how it appears in EFT's reports. The reason the last three characters and file extension are conserved is that UTF-8 and ASCII characters are identical for English characters (A-Z). So there is no loss of meaning (fidelity) after performing a UTF-8-to-ASCII conversion. This same UTF-8-to-ASCII conversion applies when EFT hands off the filename to the Event Rule dispatcher, except where an AWM action exists, in which case the filename context variable will retain the original UTF-8 encoded filename. Thus if data integration of UTF-8 encoded filenames is needed, you should consider deploying AWM tasks alongside EFT's Event Rules.

Q How do Unicode filenames appear in EFT's administration interface?

A. EFT's administration interface (AI) does not support Unicode characters. UTF-8 is always down converted to ASCII in the AI. This means you can't specify a unique UTF-8 encoded filename in EFT's offload wizard, a UTF-8 encoded username, path, or anything else for that matter. The ONLY way to process Unicode filenames in the Copy/Move and Download Actions is to use wildcards (*.*, *.dat, etc.) as the source filename, instead of using a specific filename such as梅雨右折車線.ISO.

Q. Will Unicode encoded filenames be preserved in EFT Server's context variables, such as FS.FILENAME or FS.PATH?

A. Yes and no. For all Event Rule Events, Conditions, and Actions EFT will down convert the UTF-8 characters into ASCII. The only exception is when those variables are passed to AWM. In that case alone, EFT conserves the UTF-8 encoded filename, so that AWM can consume the original UTF-8 encoded filename, as AWM is fully UTF-8 compliant.

Q. Does EFT's internal handling of the file differ depending on whether the file was received in ASCII or Unicode?

A. In the guts of EFT it handles everything in Unicode. Conversion back to ASCII occurs only when working with a system or capability that doesn't support Unicode.

Related Topics

- IDN Support in EFT
- Unicode Exceptions

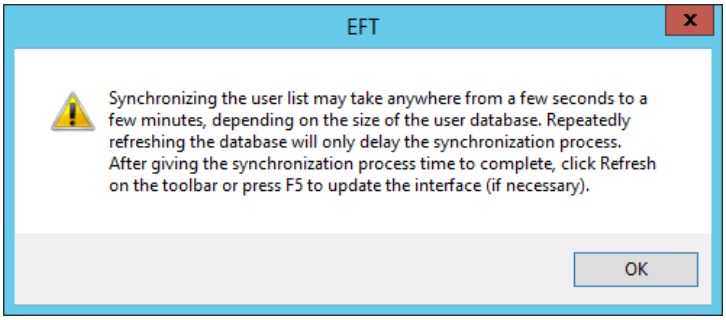
User Database Refresh

When you define EFT, you specify the refresh rate for all Sites that connect to that Server. However, you can override this refresh rate for the Site. You can also manually refresh to see any user account changes (**View > Refresh User Database**).

Database refresh should be disabled on EFT nodes used in HA configurations.

To refresh the user database

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the main menu, click **View > Refresh User Database**. A message appears explaining that synchronizing the user list might take some time.



3. Click **OK** to dismiss the message.

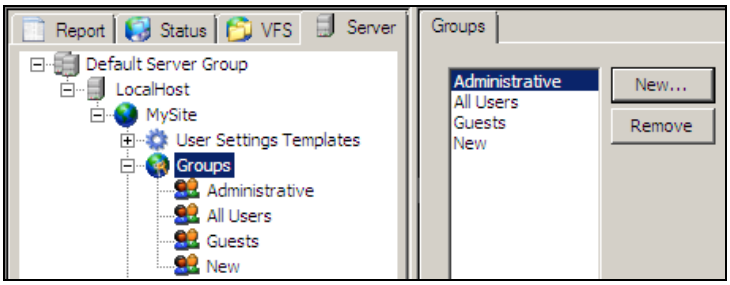
Controlling Access to Folders (Permission Groups & VFS)

The topics below provide information for creating and managing Groups in the administration interface.

- Introduction to Permission Groups
- Introduction to the Virtual File System (VFS)
- How VFS Permissions Work
- Adding a User or Group to VFS Permissions
- Adding or Removing Users to or from a Group
- Creating a New Physical Folder
- Creating a New Virtual Folder
- Creating Permission Groups
- Deleting Groups
- Deleting a Physical Folder
- Deleting a Virtual Folder
- Disabling Inheritance in the VFS
- Encrypted Folders (EFT Encryption)
- Enable EFS Encryption
- Mapping a Virtual Folder to a Network Drive
- Renaming a Group
- Renaming a Physical Folder
- Renaming a Virtual Folder
- Resetting VFS Folder Permissions
- Setting VFS Permissions
- Specify Upload Quota for Virtual Folders
- Viewing Group Membership
- WTC Users in the VFS

Introduction to Permission Groups - Controlling Access to Folders

Just as User Settings Templates control access to EFT resources such as bandwidth allowances and connectivity privileges, the Permission Groups control access to folders and the files within. Permission Groups set user virtual file system (VFS) permissions to folders. EFT creates the following default Groups for every Site: **Administrator, All Users**, and **Guests**. You can create new Groups and/or modify the settings for the default Groups. Consider your security and access needs, configure Groups according to those needs, then add users to the Groups based on the permissions that you want to allow. The **Groups**node appears in the left pane under the **Site**node on the **Server** tab. (You cannot move Groups between Sites.)

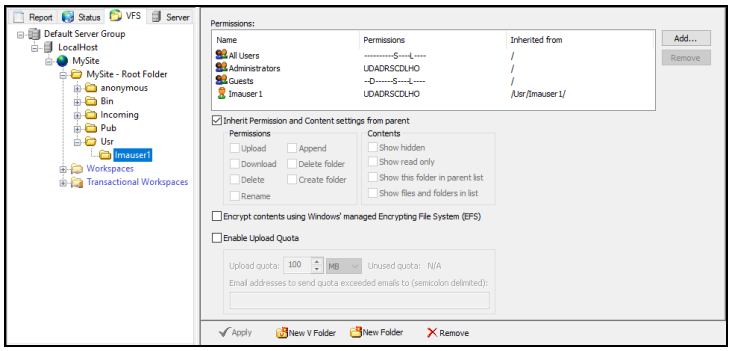


To specify user permissions

1. Create a Group(on the **Server** tab)
2. Add users to the Group (on the **Server**tab)
3. Add the Group to the **Permissions**pane (on the **VFS**tab)
4. Set the Group's VFS permissions (on the **VFS**tab)

To view Group permissions

1. In the administration interface, connect to EFT, then click the **VFS**tab.
2. In the left pane, click a folder. The default Groups appear in the **Permissions** pane. Groups that you have defined on the Site do not appear in the **Permissions**pane until you add them.



The default **All Users** and **Guests** Groups have minimal permissions; the **Administrators** Group has every permission. The letters and their organization in the **Permissions**column (UDADRSCDLHO) represent the permissions that are enabled:

U = Upload
D = Download
A = Append
D = Delete
R = Rename
S = Show this folder in parent list (show the folder selected in the left pane)
C = Create Folder
D = Delete Folder
L = Show files and folders in list
H = Show hidden (**Show files and folders in list** must be selected)
O = Show read only (**Show files and folders in list**must be selected)

If the permission is not enabled, two dashes appear instead of the letter. The default Groups have the following permissions, but you can edit them to suit your needs:

- **Administrators =**UDADRSCDLHO; every permission
- **All Users =**-- -- -- -- -- S -- -- L -- -- ; **Show folder in the parent list** and **Show files and folders in list**
- **Guests =** -- D -- -- -- S -- -- L -- -- ; **Download**, **Show folder in the parent list,**and **Show files and folders in list**

Groups can provide the permissions implied by their name (that is, the *Upload* file Permission allows users in the Group to upload files; the *Delete*folder permission allows users in the Group to delete files).

Users' permissions are inherited from the Groups to which they belong. For example, if user jsmith is a member of the **Accounting**, **All Users**, and **HR**Groups, their permissions are combined. The **Inherit**check box is not available when the root folder (for example, **MySite - Root Folder**) is selected.

For detailed descriptions of the permissions, refer to How VFS Permissions Work.

Lost Users in Permission Group

If a Site is stopped (disabled) when the EFT server service is restarted, and then the Site is started (turned on), and users are removed from all administrator-added Permission Groups. (Default Permission Groups, **Administrators, All Users**, and **Guests**, are unaffected.)

A Site's Permission Group membership is a part of the user database. To display the group's membership, EFT must synchronize with the authentication manager. Sites that are stopped are not synchronized. (EFT should not pull users from the authentication manager if the Site is disabled.)

Workaround: Synchronize the Site's user database manually after turning on the Site, or wait until the "auto-refresh" timer has fired.

Related Topics

- Creating Groups
- Deleting Groups
- Adding or Removing Users to or from a Group
- Setting VFS Permissions

Introduction to the Virtual File System (VFS)

The Virtual File System (VFS) allows you to make files and folders available to EFT users through the granting of permissions. The VFS allows you to create physical folders and virtual folders.

- **Physical folders** are folders you create on the local hard drive from EFT.
- **Virtual folders** refer (point) to existing folders on your computer or another system, similar to a Windows shortcut. Because a virtual folder name is only an alias for the real folder, when you create a virtual folder, you do not have to give it the same name as the folder it references.

On the **VFS** tab of the administration interface, you can specify which files and folders are available to users, and then specify Group and user permissions for the folders. You make the files, physical folders, and virtual folders available to users by granting permissions based on their Group membership. VFS permissions are constructed to allow users the least restrictive access to folders.

For example, suppose a user is a member of a Group that has read, upload, download, and delete permissions to a folder. Even if the user is a member of another Group that has only download permissions to the same folder, the user will be able to read, upload, download, and delete files from that folder.

User permissions are given priority.

In the folder that the user wants to access, if EFT finds user-specific permissions that are not those from Groups, EFT does not look for any Group permissions. EFT gives priority to individually configured permissions. For example, suppose there is a user with the user name Bob. Bob is a member of two permission Groups that have only download and list permissions for Folder1. However, you have decided to give Bob full permissions for Folder1 without creating a new permission Group. Because EFT looks for these individual user permissions first, then Bob will have full permissions for Folder1 no matter how his Group membership is configured. This same rule implies that if Bob has individual permissions that only allow him to download files from that particular folder, it does not matter if he is a member of two Groups that have full permissions for the folder. Bob will only have permission to download files.

If a user does not have individual permissions for a folder and is a member of more than one Group, EFT gives the user the least restrictive access for the folder.

From their Groups, users receive all the permissions available for the folder. For example, suppose a user with the user name Jan is a member of two Groups, Group1 and Group2, that both have permissions for a particular folder, Folder2. If Group1 has

download permission and Group2 has upload permission then Jan will have both upload and download permissions for Folder2.

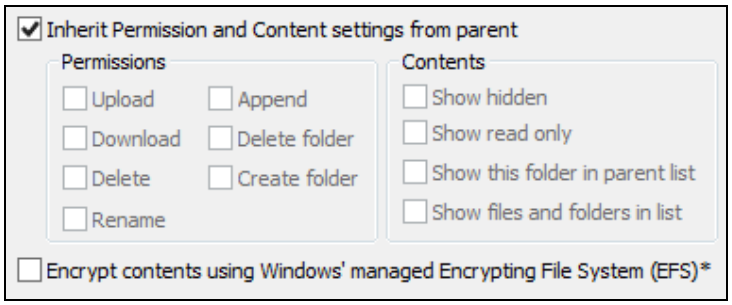
The All Users Group is the same as any other Group except that it can't be removed from the root folder permissions list.

You can use the **All Users Group** to determine inherited permissions from the parent folder. If you change any inherited permissions for the **All Users** group, EFT displays a confirmation message to make sure you want to change the inherited permissions.

EFT supports multiple concurrent administration for most setting changes but not for changes made to the VFS. This means that last committed changes will overwrite changes made by other administrators when both administrators are working from the same version of the configuration.

How VFS Permissions Work

When a user logs in to EFT's Web Transfer Client, the files and folders that the user is allowed to access depends on the permissions assigned on the **VFS**tab of the administration interface. The **VFS**tab allows you to enable or disable permissions for a group or a user as described below.



The **Inherit Permission and Content settings from parent** check box causes the selected folder in the tree to inherit the permissions assigned to its parent folder. For example, if you specify that folder Usr is to inherit the permissions assigned to its parent folder, then Usr has the same permissions as the Site root folder. If you clear the check box, a message appears in which you can copy the parent folder's permissions and then edit them as needed or remove all inherited permissions. (Refer to Disabling Inheritance in the VFS for more information about inheritance.)

The **Encrypt contents (EFS)** check box allows you to right-click a folder in the VFS tree (left pane) and encrypt the contents of the selected folder. Refer to Encrypt Data at Rest for details.

The check boxes in the **Permissions**area specify whether a user or group is allowed the permission:

- **Upload** - Allows users to upload to their folder. By default, the Administrators group and the user folders each have Upload permission. (The All Users and Guest groups do not have this permission by default.)
- **Download** - Allows users to download to their folder. By default, the Administrators group, the Guest group, and the user folders have Download permission. (The All Users group does not have this permission by default.)
- **Delete** - Allows users to delete files from the folder. By default, only the Administrators group has this permission.
- **Rename** - Allows users to rename files. By default, only the Administrators group has this permission.
- **Append** - Allows users to add to existing files after resuming an incomplete transfer. By default, only the Administrators group has this permission.
- **Delete folder**- Allows users to delete folders.
- **Create folder** - Allows users to create folders.

Contents

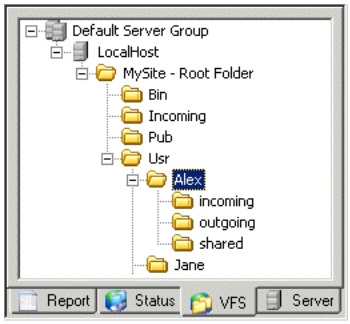
The check boxes in the Contents area specify:

- **Show hidden**- Allows users to view hidden folders and files.
- **Show read only**- Allows users to view read-only folders and files.
- **Show files and folders in list** - Allows users to retrieve a directory listing (of files and folders) from the Server. If it is not selected, no files or folders are visible. By default, only the administrators group has this permission. The **Show files and folders in list file** permission refers to the user's ability to retrieve a directory listing from EFT. If this option is enabled, the user is able to see a list

of files in the directory. If it is disabled, no files or directories will be visible. (Refer to the example below for more information.)

- **Show this folder in parent list** - Allows users to view the folder when the parent directory's listing is retrieved. The **Show this folder in parent list** permission is a bit more complex in that the permission corresponds to whether the directory is visible when a directory listing is retrieved in the parent directory. The interaction between inheritance and this setting can therefore lead to a bit of confusion. (Refer to the example below for more information.)

Within the VFS system, the **Show files and folders in list** file permission and the **Show this folder in parent list** folder permission can confuse users as to the intended operation of the server. Let's use the following folder structure as an example to explain the purpose of these check boxes.



The default folder **User** contains user folders for **Alex** and **Jane**.

If you select user **Alex** and disable the **Show this folder in parent list** permission for user **Jane**, then when user **Jane** navigates to the **Usr** directory and retrieves a directory listing, the folder **Alex**will NOT appear in her directory listing. To complicate matters, however, **Jane** still has access to the folder and if someone tells her to manually navigate to that folder, she will still be able to perform actions within the **Alex**folder (provided she has appropriate permissions). In this scenario, by default, when user **Jane** retrieves a directory listing from within the folder **Alex**, she will only see a list of files in the folder; she will not see any subfolders in the folder, because the subfolders, **incoming**, **outgoing**, and **shared**, have all inherited the disabled **Show this folder in parent list** setting.

- The **Show files and folders in list** permission applies to both files and folders in the selected directory.
- The **Show this folder in parent list** permission applies to the visibility of the selected folder in its parent directory.
- Default inheritance rules will cause the subfolders of a **Show this folder in parent list**-disabled folder to not display.

Related Topics

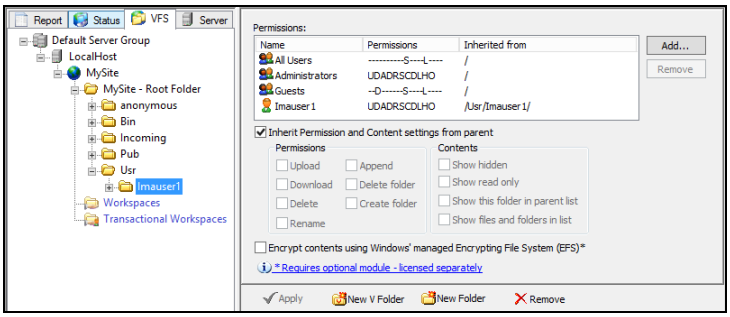
- Setting VFS Folder Permissions
- Resetting VFS Folder Permissions

Adding a User or Group to VFS Permissions

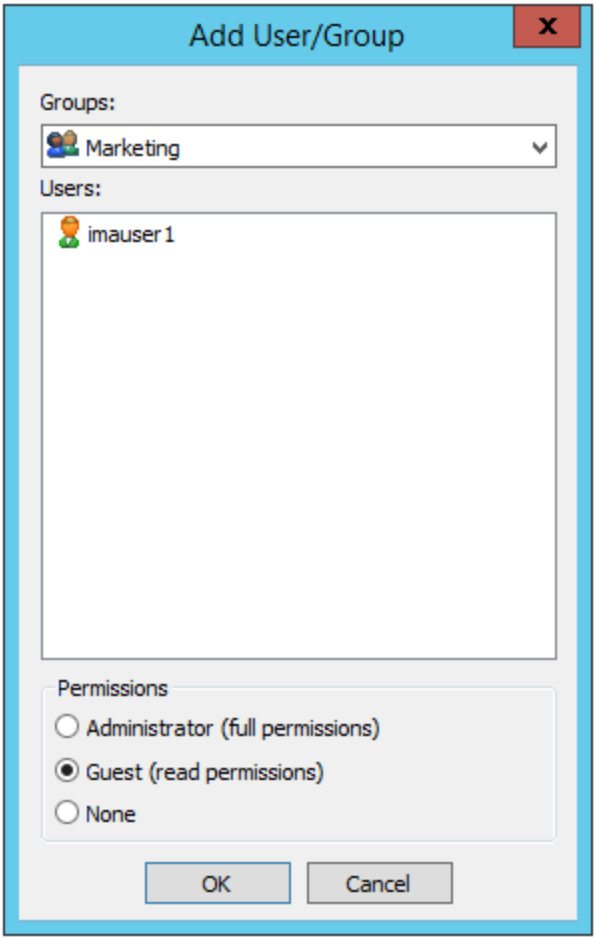
You can add a user or Group to existing permissions on the **VFS**tab's **Permission** pane. The **All Users**, **Administrators**, and **Guests** Groups are default Groups created by EFT during installation. You can create other Groups on the **Server** tab. Refer to Permission Groups for more information about Groups. (You must create the user or Group on the **Server** tab before you can add it to VFS permissions.)

To add user or Group permissions

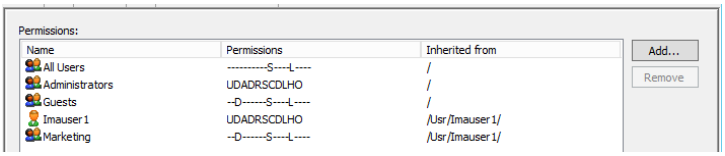
1. In the administration interface, connect to EFT, and then click the **VFS**tab.
2. In the left pane, click the folder you want to configure. The right pane displays each of the users and Groups who have permissions on the selected folder.



3. In the right pane, click **Add** or right-click a user or Group that you want to modify, then click **Add User/Group** to add a user to a Group and/or to assign their permissions on the folder that you clicked in the left pane. The **Add User/Group** dialog box appears.



4. In the **Add User/Group**dialog box, do one of the following:
   - Click the **Groups**list to specify a permission group to add the user to. Groups that you have defined on the **Server**tab appear in the **Groups**box. (Default groups do not appear, because they are already defined in the **Permissions** pane.)
   - Click the **Users**list to specify a user to add to the selected folder. Users that you have defined on the **Server**tab appear in the **Users**box.
5. In the **Permissions**area, click one of the permissions: **administrator**, **Guest**, or **None**, then click **OK**. The user or group appears in the **Permissions**pane.



6. Click **Apply**to save the changes on the server.

> **NOTE:** For information about viewing a user's VFS home folder from the **Server** tab or viewing a user's physical home folder in Windows File Explorer from the VFS tab, refer to Viewing a User's Home Folder.

Adding or Removing Users to or from a Group

When you create a user in the **Create New User** wizard, you are asked to add the user to a Group. You can later add/remove users to/from Groups on the **Group Membership** tab or Adding or Removing Users to or from a Group. You can add any user to any Group on the same Site. You cannot add users from one Site to a Group on another Site.

If a user does not have individual permissions for a folder and is a member of more than one Group, EFT gives the user the least-restrictive access for the folder. You can individually modify user permissions and those modified permissions will outweigh all Group permissions. For example, if a user is a member of three Groups that all have upload permissions to a particular folder, but you have denied that specific user permission to upload to the folder, then the user cannot upload to the folder.

To move users into or out of a group

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, expand the **Groups** node, and then click the Group you want to configure.
3. In the right pane, in the **Group Membership** tab, double-click the user or use the arrows to move the user into or out of the Group. (You can multi-select using SHIFT and CTRL.)
4. Click **Apply**to save the changes on EFT.

Related Topics

- Viewing Group Membership
- Specifying a User's Permission Group
- Creating Users
- Expiring a User Account

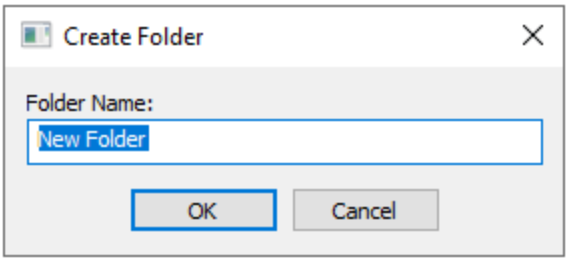
Creating a New Physical Folder

You can create a physical folder in the Virtual File System (VFS) of the administration interface.

To create a new physical folder

1. In the administration interface, connect to EFT and click the **VFS**tab.
2. In the left pane, click the folder in which you want to create a subfolder, then do one of the following:
   - Right-click the folder, and then click **New Physical Folder**.
   - On the toolbar, click the **New Folder** icon .
   - On the main menu, click **Configuration >New Physical Folder**.

   The **Create Folder** dialog box appears.



3. Type a name for the new folder, and then click **OK**. The new folder appears in the tree.

Related Topics

- Creating a New Virtual Folder
- Changing the Name of a Physical Folder
- Deleting a Physical Folder

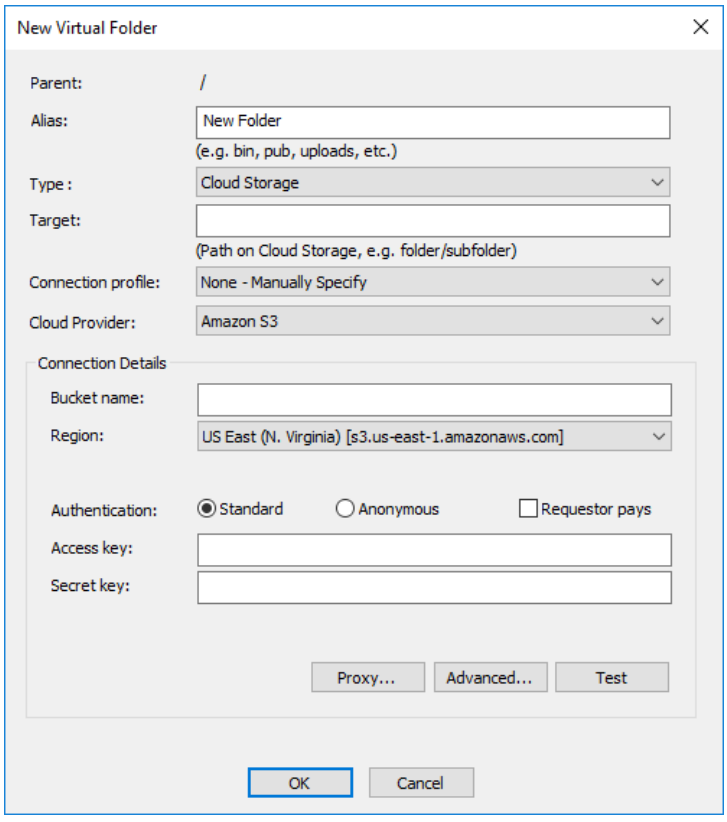
Creating a New Virtual Folder

Virtual folders reference physical folders on a computer's hard drive, LAN, or in the cloud. Similar to a Windows shortcut, a virtual folder is only an alias for the real folder. When you create a virtual folder, you do not have to give it the same name as the folder it references. You cannot change the name of a virtual folder, but you can delete the virtual folder and then re-create it with a new name.

To create a new Virtual folder

1. In the administration interface, connect to EFT and click the **VFS**tab.
2. In the left pane, click the folder in which you want to add a virtual subfolder, then do one of the following:
   - Right-click the folder, and then click **New Virtual Folder**.
   - On the toolbar, click the **New Virtual Folder** icon .
   - On the main menu, click **Configuration >New Virtual Folder**.

   The **New Virtual Folder** dialog box appears.



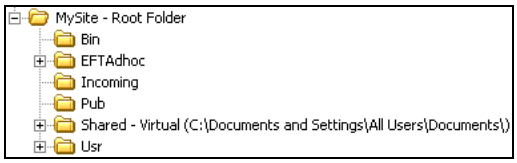
3. In the **Alias**box, type a name for the folder. For example, type `Shared`.

4. In the **Type** box, specify whether the folder is **Local/LAN** or **Cloud Storage**.

   > **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

5. In the **Target**box, specify the target folder by typing the path or click the folder icon and browse to the target folder. For example, browse to `C:\Documents and Settings\All Users\Documents\`. For cloud storage, provide the URL and/or folder ID. Please refer to Defining a Connection Profile for details.
   a. In the **Connection profile** box, click the down arrow to select a Connection Profile, if there is one defined.
   b. In the **Cloud Provider** box, click the down arrow to specify **Amazon S3**, **Amazon S3-compatible**, **Azure blob storage**, or **Azure Data Lake Storage gen 2**. then configure the **Connection Details** accordingly.
   c. For **Proxy** and **Advanced** configuration, refer to Defining a Proxy and Specifying Advanced Transfer Options.
6. Click **OK**. The new virtual folder appears in the tree with the name that you typed in the **Alias** box, plus "Virtual" and the full path. For example:

```
Shared
 - Virtual (C:\Documents and Settings\All
Users\Documents\).
```



For cloud storage, the VFS name appears as "Alias - Virtual (Type://Info/Target)", where:

- Alias = name of folder
- Type= S3\Azure\CP (Connection Profile)
- Info = short details of Storage or Connection Profile name
- Target - relative path on Storage.

Related Topics

- Creating a New Physical Folder
- Deleting a Virtual Folder
- Mapping a Virtual Folder to a Network Drive
- Defining a Connection Profile

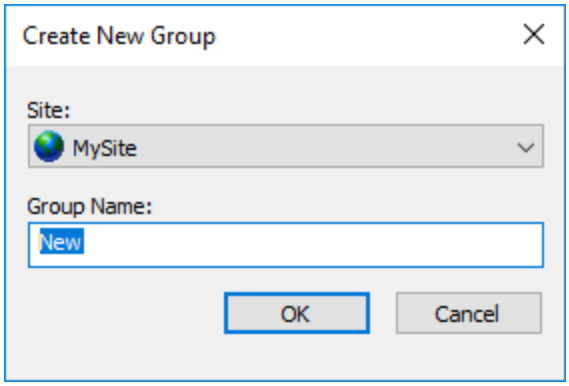
Creating Permission Groups

You can create a permission Group and add any users from the Site to a Group. You can then grant permission to folders by Groups rather than granting permissions to each individual user. Refer to Deleting Groups for information about deleting a Group.

To create a permission Group

1. In the administration interface, connect to EFT and click the **Server**tab.
2. Do one of the following:
   - Press CTRL+G.
   - Right-click in the left pane, and then click **New Permission Group**.
   - On the main menu, click **Configuration**, and then click **New Permissions Group**.
   - On the **Server**tab, click the **Groups**node, then in the right pane, click **New**.

   The **Create New Group** dialog box appears.



3. In the **Site**box, click the list to specify the Site for which you want to create the new Group (if you didn't click the **Groups**node in a Site tree).
4. Type a name for the Group in the **Group Name** box. For example, type `R&D`. The **Group Name** can contain up to 255 characters.
5. Click **OK**. The new group appears under the specified Site in the **Groups**node.

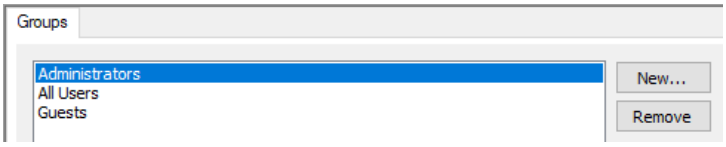
Refer to Adding or Removing Users to or from a Group and The Virtual File System for information about users' permissions in relation to their assigned Group(s).

Deleting Groups

Deleting a Group does not delete the users assigned to that Group. You cannot delete the **All Users** Group.

To delete a group

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Groups** node.
3. Expand the **Groups**node, click the Group you want to delete, and then click the Delete icon ✕ or press DELETE on the keyboard.
4. In the right pane, click the Group that you want to delete, and then click **Remove**.



   A confirmation prompt appears.

5. Click **Yes**. The users in the deleted Group retain membership in any other of their assigned Groups and the **All Users** Group.

Related Topics

- Permission Groups
- Creating Groups
- Adding or Removing Users to or from a Group

Deleting a Physical Folder

When you delete a physical folder from within EFT, the folder is deleted from EFT AND your computer's hard drive. If you want to delete only the reference to the folder in EFT, refer to Deleting a Virtual Folder.

To delete a physical folder

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, right-click the folder you want to delete, and then click **Delete Folder**. A confirmation message appears.
3. Click **Yes**.

Related Topics

- Creating a New Physical Folder
- Changing the Name of a Physical Folder
- Creating a New Virtual Folder
- Deleting a Virtual Folder

Deleting a Virtual Folder

When you delete a virtual folder, you merely delete a pointer, not the actual folder it references. (If you want to delete the physical folder and everything it contains from the hard drive, refer to Deleting a Physical Folder.)

EFT does not allow removal of the system-created folders **Bin**, **Pub**, and **Usr**, because user folders are saved in these folders.

To delete a virtual folder

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, right-click the folder you want to delete, and then click **Delete Folder**. A confirmation message appears.
3. Click **Yes**.

Related Topics

- Creating a New Virtual Folder
- Deleting a Physical Folder
- Mapping a Virtual Folder to a Network Drive

Disabling Inheritance in the VFS

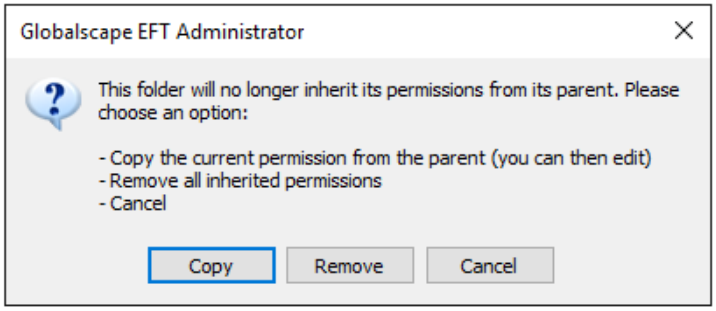
You can override a user's inherited settings by clearing the **Inherit permissions from parent folder** check box. If you later decide you want the folder to inherit permissions again, simply select the **Inherit permissions from parent folder**check box.

The following procedure describes how to prevent a folder from inheriting its parent folder's permissions and force a single modified folder to begin inheriting permissions to sub-folders.

To reset all subfolders of a particular parent folder to inherit permissions from that parent, refer to Resetting VFS Folder Permissions.

To stop or force a folder from inheriting permissions

1. In the administration interface, connect to EFT and click the **VFS**tab.
2. In the left pane, click the folder you want to configure.
3. In the right pane, do one of the following:
   - To force the selected folder to inherit permissions from a parent folder, select the **Inherit permissions and Content settings from parent folder** check box.
   - To stop the selected folder from inheriting permissions from a parent folder, clear the **Inherit permissions and Content settings from parent folder** check box. A message appears.



4. On the message that appears, click one of the following:
   - **Copy** - duplicates the permissions of the parent. You may later edit the permissions.
   - **Remove**- deletes all inherited permissions
   - **Cancel**- aborts the changes and closes the message

Encrypted Folders (EFT Encryption)

EFT Server provides the following forms of securing files on disk (data-at-rest encryption):

- OpenPGP-based encryption is a well-known, dual-key based encryption technology. The primary benefit is the fact that only recipients whose public key was included at the time of encryption will be able to decrypt the file, assuming they own the corresponding private key to their public one. This provides more control over who can access the data, vs. other methods. PGP has two shortcomings: First, it requires that participants create and maintain their key pairs, adding complexity to the process. Second, it is not a streaming encryption technology, as the entire file must be present (written to disk) before encryption (or decryption) can occur. In the context of file transfers, the result is temporary files that cause havoc with automation that consumes files the moment they are received in the target directory. Refer to OpenPGP and EFT for how to use OpenPGP.
- Integrated Windows encryption via Encrypted File Share (EFS) addresses all of the drawbacks of PGP, eliminating participant key management and providing streaming encryption at the file I/O level; however, it also suffers from two shortcomings: First, some network drive technologies do not support Windows EFS (turning it on in EFT has no effect). Second, standards such as PCI DSS disallow the use of encryption technologies where the keys required for encryption/decryption reside on the systems within PCI scope. It just so happens that Window's EFS keys do reside on the target system. Refer to Enable EFS Encryption for how to use Windows EFS integration.
- Encrypted folders(EFT built-in encryption) provides an alternative to using a best-of-breed 3rd party data-at-rest encryption solution. EFT's encrypted folders provide streaming encryption (and decryption), enabling transparent, seamless file read/write. The symmetric encryption leverages AES 256 in CTR mode, with the encryption key known only to EFT. Any file touched by EFT's protocols (either as a server or as a client) are automatically encrypted (or decrypted) on arrival or departure, as appropriate. In SSL FIPS mode, encryption at rest uses the FIPS-certified SSL library.

  The primary drawback to the built-in encryption feature is that fact that any side-channeled files, such as those directly copied into a folder designated as an encrypted folder, will not be encrypted or decrypted by EFT. In fact, if you place a plaintext file in an encrypted folder and a customer logs in and downloads the file, the file will be corrupted, as EFT will attempt to decrypt what it thinks is an encrypted file. This risk can be mitigated by never side-

channeling files into folders designated as secure. Instead, use EFT's event rule Copy/Move-> LAN copy action to move files from network shares or physical folders into the secure target, as that will result in the content being encrypted (or decrypted, if done in the other direction).

> **NOTE:** Encrypted folders with long paths are not supported. (TFS389235)

- **Encrypted Folders Command-Line Utility** - EFT's built-in folder encryption feature will encrypt files as they arrive or decrypt them as they leave EFT via standard protocols; however, there may be instances where you need to encrypt or decrypt files independent of EFT, while adhering to the same encryption mechanisms (AES-256 symmetric-key). For example, you may want to encrypt a file received by a folder monitor rule, or conditionally encrypt files prior to emailing them, or decrypt previously encrypted files side-channeled into EFT from a different EFT server. To that effect, EFT's encryption/decryption subroutines have been exported to a command utility, **eftencrypt.exe**, which is installed alongside EFT in the **\Redistributables** subfolder. You can run the utility directly or from within EFT's Event Rules, by leveraging the built-in PowerShell action. You can also copy the utility to another computer to encrypt and decrypt files there. (The utility follows standard command line rules.)

To use the eftencrypt.exe utility

1. Locate the **eftencrypt.exe** utility. (The default is **C:\Program Files\Globalscape\EFT Server**)
2. Locate your Site or specific Encrypted Folder's encryption key. Alternatively, create a new 256-bit key (64 hexadecimal characters, i.e. 32 bytes in length).
3. Locate the name of the target file you want to encrypt or decrypt.
4. Launch a command line prompt or PowerShell, running as Administrator. Alternatively, create a PowerShell action in EFT's event rules.
5. To encrypt or decrypt in place, type: eftencrypt.exe <key> <path to target file>
6. To encrypt or decrypt using source and destination: eftencrypt.exe <key> <path to source file> <path to target file>

Each of these methods has benefits and drawbacks. Other alternatives include using third-party data-at-rest encryption, such as the built-in encryption provided by some NAS devices.

EFT provides an advanced property, **IgnoreEncryptedFoldersInOutboundTransfers**, which can be used to prevent EFT from decrypting encrypted folders during transfers. For example, EFT receives a file into an encrypted folder and EFT encrypts it. Then the file is transferred to another system using EFT's "Copy/Move" event rule action, which normally results in the file being decrypted. If the advanced property **IgnoreEncryptedFoldersInOutboundTransfers** is set to True, the file will remain encrypted when transferred. It can then can be decrypted later with the **eftencrypt.exe** utility.

EFT Built-In Encrypted Folders

Physical folders can be transparently encrypted during read/write using EFT-managed AES-256 *symmetric encryption* (CTR mode), which uses a secret key known only to the server. The server will encrypt files as they arrive over supported protocols, and decrypt files when departing over those same protocols. The server, when acting as a client, will also encrypt files that it downloads into an encrypted folder, and decrypt files that it copies or moves to a remote server, including LAN copy. (See below for instructions for creating the key.)

- EFT randomly generates the Encrypted Folders key upon new Site creation. You should change the secret and maintain a copy of the secret in your key manager.
- If the Advanced Property **EncryptedFolderKey**is defined and not malformed, EFT uses it for encryption/decryption, read at service startup. (This is mainly for EFT upgrades to 8.0.4 from earlier builds. The key can be created/edited in the **Encrypted folders** dialog box, as described below.)

- Upon EFT upgrade, EFT generates a new key if the key is the old "default" value, and no other key is defined
- Per-folder encryption keys can be used to encrypt the contents of all data in the site root automatically, using a separate key for each sub-folder off of the site root, and also for folders referenced by virtual folders (VFS) that are shared by users.

The following considerations for encrypted folder targets should be noted:

- Encrypted folders are limited to physical folders (Per-folder encryption keys can be used on physical folders referenced by virtual folders.)
- Encrypted folders affect subfolders within the designated folder
- Encrypted folders can only point to folders that are under the Site root (for example, **C:\InetPub\EFTRoot\MySite**)
- When using Encrypted folders, you can only encrypt files in the directory hierarchy of the Site's root folder. Make sure that the Site root folder on the **Site > General** tab is pointing to the correct path. That is, if the HA config drive is **D:\HAConfig\,** you should edit the Site root folder to point to **D:\HAConfig\InetPub\EFTRoot\MySite**.
- Encrypted folders cannot be EFT system folders (Install Folder, App Data Folder, Cluster Share) and Windows reserved directories (Windows, ProgramData, ProgramFiles, ProgramFilesx86), or their parents or children, and cannot be specified even by server administrators. This is includes subfolders of those folders.
- When configuring network shares for data encryption, the EFT service account must have access to the encrypted folder path; otherwise, you will be presented with a failure
- Using the CIC Action with encrypted files will not return an accurate result. Copy/move the files to a folder that is not encrypted to process with the ICAP server.
- If you are remotely connected via the administration interface, you will not be able to browse for folders. Instead, you must specify a valid, approved path, local to the server.
- Whether local or remotely connected via the administration interface, administrator accounts beneath the role of Server administrator (that is, Site administrator and below) will not able to browse for folders. Instead, these administrators must specify a valid, approved path, local to the server.
- If the server cannot perform initial encryption or final decryption due to lack of permissions, sharing violations, or network disconnect, a warning will appear indicating that "Some files in the folder were not [encrypted|decrypted]. The data in the folder might be corrupt."

- The following protocols and protocol commands are encryption/decryption aware:
  - EFT FTP/HTTP/SFTP Server (Listening Engines): all operations: upload, download, resume, FTP COMB, FTP and HTTP XCRC32, HTTP Copy file, HTTP/FTP/SFTP move file/folder, HTTP ZIP Folder Download.
  - EFT FTP/HTTP/SFTP/Local Transfer Client (Client FTP transfers): offload, download, resume, Pre/Post commands, "Rename To" after download, FTP data integrity check (CRC).
- All side-channel operations and all actions outside of copy/move/download are unaware of encryption/decryption. So if, for example, you have a Timer rule that downloads a file from a remote host, to an encrypted folder, and then a subsequent action attempts to manipulate that file (for example in Advanced Workflows), that file could be encrypted, and thus Advanced Workflows will not be able to parse it.
- A new logger is available in Logging.cfg for output to EFT.log, labeled EncryptedFolders, set to TRACE by default.
- COM support is available
- You can only encrypt the folders in the Site's root folder. If you attempt to encrypt folders outside of the EFT Site's root folder (for example, C:\InetPub\EFTRoot\MySite) an error prompt occurs: "This folder is not in the directory hierarchy of this Site's root folder."
- EFT system folders (Globalscape/EFT, AppData, and cluster share) and Windows reserved directories (Windows, ProgramData, ProgramFiles, ProgramFilesx86), as well as their parents or children, cannot be encrypted. If a reserved path is selected in the**Folder to Encrypt** dialog box, an error prompt occurs: "This is a reserved path and cannot be encrypted."
- Before you enable this feature, it is recommended that you set up appropriate backup measures to protect your data. If you need to recover a private key to decrypt data, and that key is lost, you will not be able to recover the data that the key protects. If you need more information on setting up appropriate backup procedures, refer to Configuration and Security Best Practices.
- If you had used the Encrypted Folder Key advanced property in versions prior to v8.0.4, the property for the key will appear in the AdvancedProperties.json file. EFT only uses that advanced property for backwards compatibility. After upgrading, if you want to change the key you should do so in the EFT administrator interface, NOT via the advanced property.
- The following scenarios represent the only way in which files get ENCRYPTED when interacting with an encrypted folder:

    - When files are uploaded to EFT via HTTP/FTP/SFTP into an encrypted folder.
    - When files are downloaded by EFT (via a download action) via all protocols including LAN, from a remote server into an encrypted folder.
        - Likewise when using EFT's synchronize action (make local just like the remote), when downloading to an encrypted folder.
    - When PGP action writes file to an encrypted folder. The file is first PGP encrypted then AES-256 encrypted in a streaming fashion.
- The following scenarios represent the only way in which files get DECRYPTED when interacting with an encrypted folder:
    - When files are downloaded from EFT via HTTP/FTP/SFTP. The file is decrypted before it is sent down the wire.
    - When files are uploaded (offloaded) by EFT (via copy/move action) via all protocols including LAN, to a remote server.
        - Likewise when using synchronize action (make remote appear as local), when uploading from an encrypted folder.
    - When PGP action reads a file from an encrypted folder. The file is first AES-256 decrypted, then PGP decrypted in a streaming fashion.
- The advanced property **IgnoreEncryptedFoldersInOutboundTransfers** is used to prevent EFT from decrypting encrypted folders during transfers. For example, EFT receives a file into an encrypted folder and EFT encrypts it. Then the file is transferred to another system. If the advanced property **IgnoreEncryptedFoldersInOutboundTransfers** is true, the file remains encrypted when transferred. It can then can be decrypted with eftencrypt.exe. Use eftencrypt.exe <key> <path to target file> to run the decryption process, and then file is decrypted.

Site Encryption

You can encrypt all folders under the Site root using a single, reusable key for encrypting and decrypting data. EFT will encrypt all data in that folder and its subs using the Site encryption key. Subsequent files written to those folders by users uploading files will result in those files being encrypted with the site encryption key automatically and transparently. Event Rules that process files written into those folders will decrypt using the site encryption key. (Refer to Enabling EFT-Managed Encryption, below.)

Per-Folder Encryption

If you want to encrypt the contents of all data in the Site root, you can use a separate key for each sub-folder under the Site root, and also for physical folders pointed to by virtual folders (VFS) that are shared by users.

1. In the **Folder to encrypt** dialog box, add each sub-folder under the Site root folder, and then assign it a per-folder encryption key, as described in Enabling EFT-Managed Encryption, below. For example:
2. EFT encrypts all data in the specified folders and sub-folders using the corresponding folder encryption key.
3. Subsequent files uploaded to those folders by users will be encrypted with the corresponding folder encryption key.
4. Event Rules that process files written into those folders will decrypt the files using the folder encryption key.

User-Specific Encryption

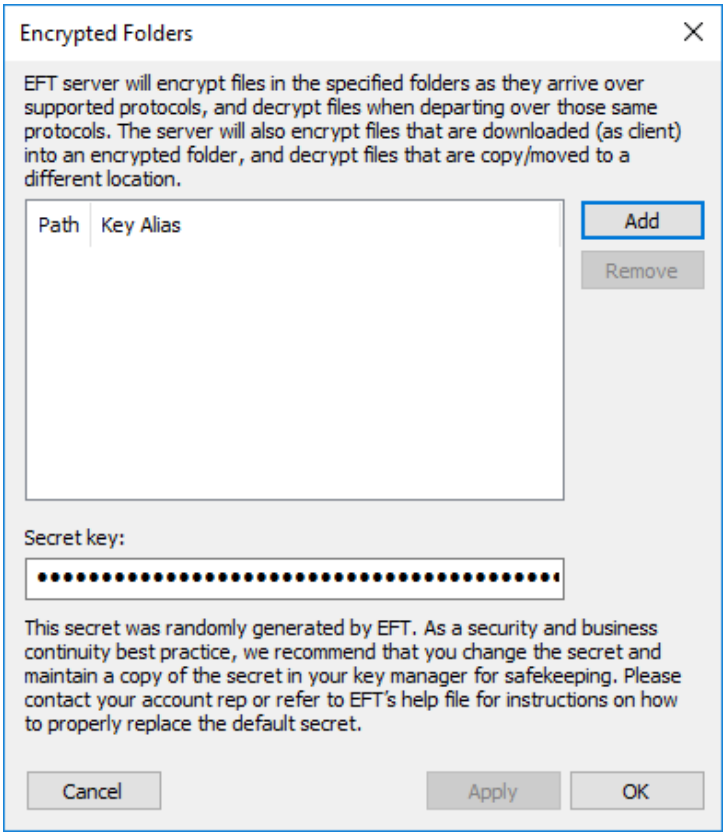
If you want to encrypt the contents of all data in the Site root, and also want to use a user-specific encryption key.

1. In the **Folder to encrypt** dialog box, click the folder icon to select a user's home folder.
2. Click **Use unique encryption** key and provide a key from the user's password manager.
3. **Click** OK.
4. EFT will encrypt all data currently in that folder and its sub-folders, including any physical folders pointed to by virtual folders, using the corresponding folder encryption key.
5. Subsequent files written to those folders by users uploading files will result in those files being encrypted with the corresponding folder encryption key.
6. Subsequent physical folders added by the user or admin or physical folders added by nature of a new virtual folder being associated with that user will results in their newly added contents also being encrypted.
7. Event Rules that process files written into those folders will decrypt using the corresponding user encryption key.

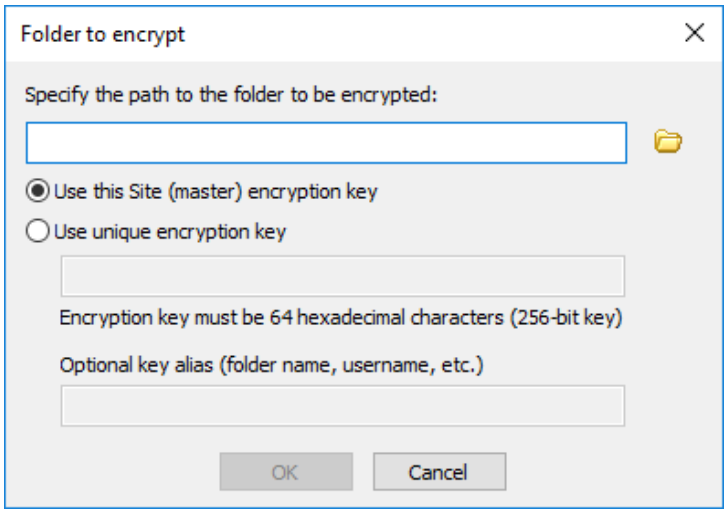
Enabling EFT-Managed Encryption

To enable EFT-managed encryption

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Security** tab.
4. In the **Data Security** area, next to **Encrypted folders**, click **Configure**. The **Encrypted Folders** dialog box appears.



   - Set the value to a string of exactly 64 hexadecimal digits (that is, 0-9 and A-F)
   - This value is not used if the value is blank or malformed (for example, if you have more or less than 64 digits)
   - Restart the EFT server service for the new key to take effect.
   - In an HA or Disaster Recovery scenario, each EFT must share the same key.
5. To add folders that contain files you want to encrypt, click **Add**. The **Folder to encrypt** dialog box appears.



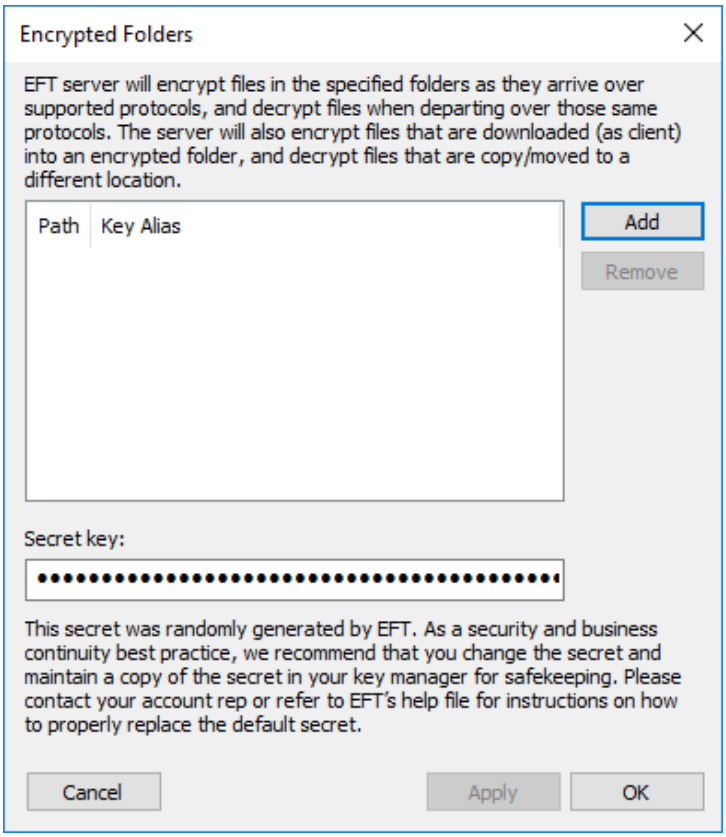
6. Type or browse for the folder that you want to encrypt. You can only encrypt the folders in the Site's root folder (for example, C:\InetPub\EFTRoot\MySite). (See note above regarding clusters.)
7. Click one of the following:
   - **For the Site encryption key**, click **Use this Site (master) encryption key** (the default).
   - **For per-folder encryption**, click **Use unique encryption key**, then paste or type the key (64 hexadecimal characters, 256-bit key). Optionally, provide an alias for this key. Note that using the same alias more than once does not cause a prompt, warning, or error. You can provide anything you want as an alias. The alias is purely for you to identify keys. If you want to use the same alias or no alias, you can. (However, providing the same alias for more than one key defeats the purpose of providing the alias.)

   Files uploaded to this folder will be encrypted upon arrival and decrypted upon departure over EFT's supported protocols. EFT will also encrypt files that are downloaded (as client) into an encrypted folder, and decrypt files that are copied or moved to a different location.

   EFT will attempt to decrypt any and all files already present in the folder. (This may take a long time if there are many files in the folder.)

To remove or replace an encrypted folder from the list

1. On the **Site > Security**tab, click **Configure** next to **Encrypted folders**. The **Encrypted Folders** dialog box appears.



- If the **Folder Path**list is empty, then the password field is NOT read only (that is, you can change the key).
- If the **Folder Path**list is NOT empty, select a folder in the list of folders, then click **Remove**. All encrypted files in the "removed" folder will be decrypted. (This may take a long time if there are many files in the folder. Note that files are not deleted, just unencrypted.)

2. In the **Secret key** box, provide a new key, then add the folder(s) back to the dialog box to be encrypted.
3. Click **OK** to close the dialog box, then click **Apply**.

Related Topics

- Personal Data Encryption
- Privacy Configuration

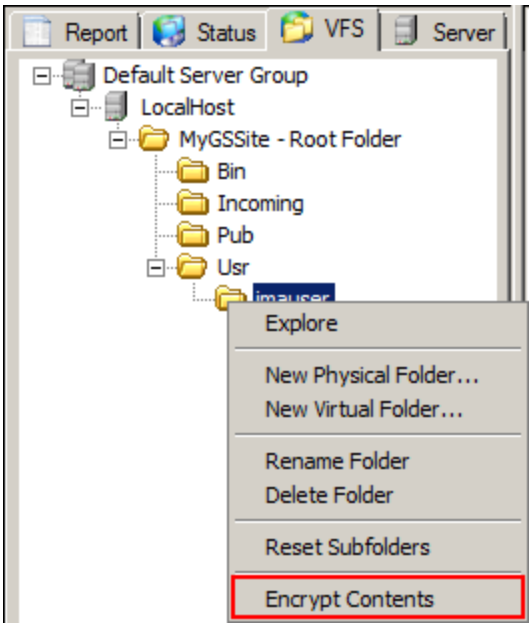
EFS Encryption

Physical folders stored on the disk in EFT's Virtual File System (VFS) can be transparently encrypted during read/write using Microsoft's Encrypting File System (EFS) by which data is encrypted as it is written to disk, and decrypted prior to transmission.

- Before you enable this feature, it is recommended that you set up appropriate backup measures to protect your data. If you need to recover a private key to decrypt data, and that key is lost, you will not be able to recover the data that the key protects. If you need more information on setting up appropriate backup procedures, refer to Configuration and Security Best Practices.
- When EFT is running in HA mode and sharing a network resource, you must run the EFT server service with a Log On account that can access that shared network resource.
- EFS is not available for systems running on FAT32 file systems. NTFS is required.
- EFS is not available with NT authentication due to limitations of NT authentication. If you require this feature with an NT set up, LDAP authentication is recommended.
- The PCI DSS requires that logical access and decryption keys be managed independently for disk-level encryption. If you enable this EFS for a high security-enabled Site, EFT prompts you to disable it, or continue with reason.
- The PCI DSS requires that if EFT disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts. That does not mean EFS cannot be used at all, but rather that it cannot be used as the sole mechanism for repository encryption. For this reason, the Server will only warn, rather than fail, during an audit.
- If you have a large number of VFS folders and the interface becomes unresponsive when EFS is enabled, be sure to clear the EFS folder icon check box. Selecting the **Enable EFS folder icons**check box when you have a large number of VFS folders can cause the interface to become unresponsive while the server checks each one for encrypted contents.
- You cannot have the folder open when trying to encrypt the folder in EFT.

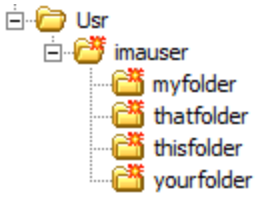
To enable EFS encryption

1. In the administration interface, connect to EFT and click the **VFS**tab.
2. In the left pane, right-click the parent folder you want to configure, and then click **Encrypt Contents**.



3. If the folder you selected has subfolders, a confirmation message appears.

4. Specify whether to **Apply changes to this folder only** or **Apply changes to this folder and all subfolders**, and then click **OK**.
   - If the Enable EFS folder icons check box is selected, the encrypted folder and subfolders display a red asterisk to indicate that the folder contents are encrypted.



5. To remove encryption, right-click the encrypted folder and click **Encrypt Contents**to clear the check box.

6. If the folder you selected has subfolders, a confirmation message appears. Specify whether to **Apply changes to this folder only** or **Apply changes to this folder and all subfolders**, and then click **OK**.

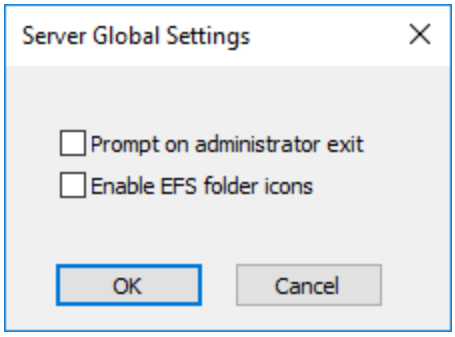
Enable EFS Folder Icons

When EFS is applied to a folder, you can configure the Server to add a red asterisk to the folder icon to indicate that the folder contents are encrypted. This setting is turned off by default. If you select the **Enable EFS folder icons** check box, the server will check each folder for encrypted contents before displaying the icon.

If you have thousands of folders, you should leave the check box unselected; selecting the check box when you have a large number of folders can cause the interface to become unresponsive while the server checks each one for encrypted contents.

To enable the EFS folder icons

1. On the main menu, click **Edit > Global Settings**.



2. Select the **Enable EFS folder icons** check box.
3. Click **OK**. (To disable the feature, clear the check box.)

Related Topic

- Encrypted Folders (EFT Encryption) with EFT-managed encryption

Mapping a Virtual Folder to a Network Drive

To map a virtual folder to a network drive, you need to:

- Establish a separate Windows account for the EFT service.
- The account must have full access to any folder you want to make available on EFT.
- Your account on the computer on which EFT is running must have full access to any folder you want to make available on EFT.

To map to a network drive

1. Create and assign a Windows account on the computer on which the **EFT** service is installed.

   This should not be the default (system) account.

2. Assign restrictive file and folder permissions for this account.
3. If you are mapping to a network drive in a workgroup, create a matching account on the target remote computer. Make certain it uses the SAME user name and password. Restrict permissions to this account to allow users access to only the folders they need.
4. In the administration interface, connect to EFT, and then click the **Server** tab.
5. Create a virtual folder for a folder on your networked drive. If you are administering remotely or the drive is not mapped to your computer, ***make sure that you use a UNC path name***.
6. In the administration interface, assign permissions for users by clicking the **VFS** tab, clicking the folder to which you want to specify the permissions for that user, and then selecting or clearing the appropriate permission boxes.

To create accounts, you need administrative rights to the system on which the service is running.

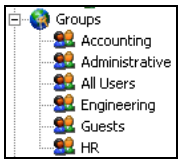
Virtual folders that point to a drive other than C: or a UNC share are visible using the MLSD FTP command.

Renaming a Group

When you rename a permission Group, all references to the Group are also updated.

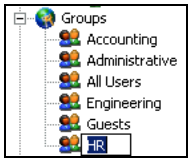
To rename a permission Group

1. In the administration interface, connect to EFT and click the **Server**tab.
2. Expand the **Site**node, then expand the **Groups**node.



3. Click the Group that you want to rename, then do one of the following:
   - Click the name. (Do NOT double-click.)
   - Right-click the name, and then click **Rename**.
   - On the main menu, click **Configuration > Rename Selected**.
   - Press F2.

   The name will become an editable text box.



4. Type the new name in the text box, then press ENTER or click away from the box. The **Groups**node will automatically resort alphabetically.

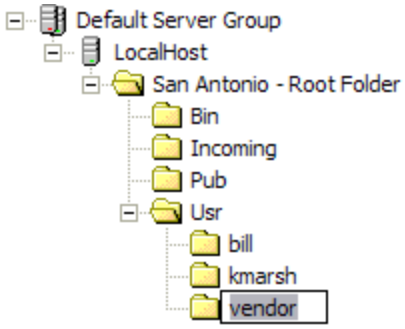
Renaming a Physical Folder

You can change the name of a physical folder in the VFS tree.

Refer to File-Naming Conventions for more information about special characters in file names.

To rename a physical folder

1. In the administration interface, connect to EFT and click the **VFS** tab.
2. In the left pane, right-click the folder you want to configure, and then click **Rename Folder**. The folder name becomes an editable text box.



3. Provide the new name, then press ENTER.

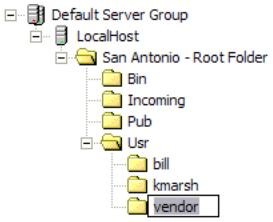
Renaming a Virtual Folder

You can change the name of a virtual folder in the VFS tree.

> **NOTE:** When renaming a virtual folder, do not include the path suffix that appears after the name. For example, to rename "Test - Virtual (CP://AWS Cloud Profile/" to "Final" the resulting name should be only "Final" without the suffix (- Virtual (CP://AWS Cloud Profile/). Adding the disallowed characters, (:// will cause the renaming to fail.
>
> Refer to File-Naming Conventions for more information about special characters in file names.

To rename a folder

1. In the administration interface, connect to EFT and click the **VFS**tab.
2. In the VFS tree (left pane), right-click the folder you want to configure, and then click **Rename Folder**. The folder name becomes selectable.



3. Provide the new name, then press ENTER.

Resetting VFS Folder Permissions

When you reset permissions on a parent folder, you force the subfolders to mirror the parent folder's permissions. This simplifies the permissions status of these folders, making them more predictable.

Resetting folder permissions from a parent folder differs from manually changing the inheritance values of subfolders. In a subfolder, you have the option either to mirror the parent folder's permissions or to keep permissions for any new users and Groups you have added while also mirroring the permissions for all Groups in the parent folder.

To reset folder permissions from a parent folder

1. In the administration interface, connect to EFT and click the **VFS**tab.
2. In the left pane, right-click the parent folder you want to configure, and then click **Reset Subfolders**.
3. Click **OK**.

Related Topics

- Setting VFS Folder Permissions
- Modifying VFS Permission

Setting VFS Permissions

After you create a Group, you add users to the Group, then on the **VFS**tab you add the Group to the **Permissions** pane, and then set the Group's VFS permissions. You can set permissions by Group or per user. If you specify a home folder when you create a new user, the user has full permission on that folder. Refer to Introduction to the Virtual File System (VFS) and How VFS Permissions Work for details of how virtual folder permissions work.

Any time a new folder is created, it inherits permissions from its parent folder. Using permission inheritance, administrators can make global access changes by simply changing group access in a parent folder. You can modify a folder's permissions even while it is inheriting permissions from a parent folder.

You can specify different permissions for child folders, rather than inheriting all permissions from the parent. When you select or the clear the check box for one or more permissions on a parent folder, and then click **Apply**, a message appears asking whether you want to apply the changes to the child folders also.

- Click **Yes** to apply the permissions to each of the child folders or **No**if you only want the permission to apply to the parent folder. You can then, if you so choose, set folder permissions for the subfolders independently of the parent folder.

To set folder permissions

1. In the administration interface, connect to EFT and click the **VFS**tab.
2. In the VFS tree (left pane), click the folder you want to configure. The **Permissions**area in the right pane displays each of the users and Groups who have permissions defined for the selected folder.
3. In **Permissions**area in the right pane, click the user or Group you want to modify or click **Add** to specify permissions for a user or Group on the selected folder. Refer to Adding a User or Group to VFS Permissions for the procedure for adding a user or Group.
4. Select or clear the appropriate permission check boxes.

   Modifying a permission affects all subfolders containing the user or Group for which the **Inherit permissions from parent folder** check box is selected.

5. Select the **Encrypt contents (EFS)** check box. Refer to Encrypt Data at Rest for more information.
6. Click **Apply**to save the changes on EFT.

Related Topics

- Resetting VFS Folder Permissions
- Encrypt Data at Rest

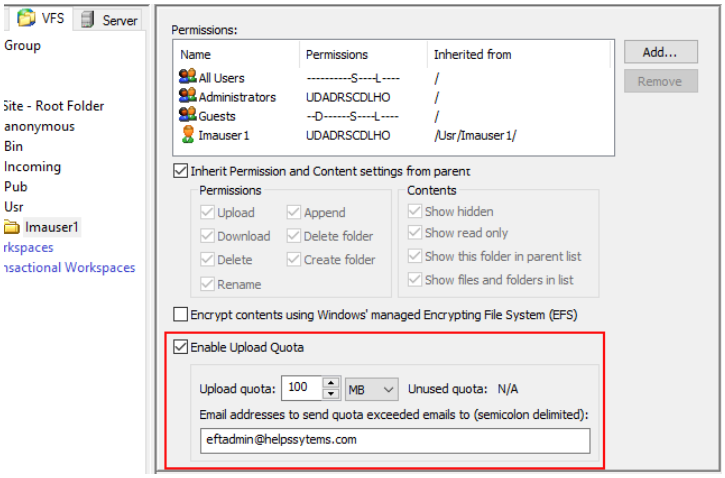
Specify Upload Quota in the VFS

Unlike User quota, *Upload* quota is set at the VFS folder level and is measured based on traffic into the VFS folder, not the size on disk. Upload quotas can be configured at the root level or subfolder, but not both. The upload quota is then inherited to subfolders. Upload quota is specific to the transfers that occur into the server. Additionally, it is not based on a per user transfer and instead collectively captures the quota for the VFS folder via the various protocols.

The EFT administrator can specify an upload quota for virtual folders. The quota applies across clusters and applies to all protocols.

To specify an upload quota

1. In the administration interface, connect to EFT and click the **VFS**tab.
2. In the left pane, click the folder for which you want to specify a quota.



3. In the right pane, select the **Enable Upload Quota** check box.
4. Next to the **Upload quota** box, specify the quota.
5. Click the drop-down box to specify MB, GB, or TB.
6. In the **Email addresses to send quota exceeded emails**, provide 1 or more emails, separated by semicolons.
7. Click **Apply**.

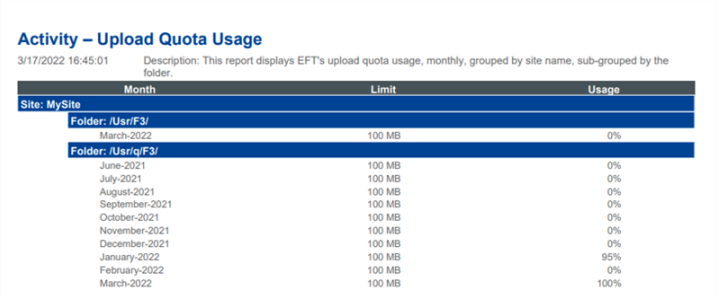
Additional information about VFS upload quota

- An advanced property (AP), **UploadQuotaUpdateIntervalSecs**, is available to specify the interval in seconds for upload quota updates to persist and propagate across HA cluster; default = 3 seconds.
- Uploads from these protocols are allowed: HTTP/S, SFTP, FTP/S, AS2

- Usage count persists through server restarts
- Usage count resets at the end of the calendar month
- EFT will remember the last changed upload quota in the registry and reuses it as the default for the folders for which the quota has not been specified, so admin can use same upload quota for mass quota management routine.
- Quotas can be changed at any time and take effect immediately; current usage counts are not affected
- Quotas are not allowed on subfolders when the parent folder has an upload quota enabled
- If quota is enabled on a folder, the quota option is disabled for all subfolders
- If quota is already turned on for a folder(s) and quota is then turned on for a parent folder the admin is notified that existing subfolder(s) quota(s) will not be enforced; the advisory will include all VFS subfolders that have quotas and allow the administrator to cancel the action.
- If an upload will cause the quota to be exceeded, the upload will fail with an error code for the protocol:
    - HTTP/S/AS2 – Error code 403
    - FTP/S – Error code 552
    - SFTP - Error code 15
    - For SFTP/FTP protocol – Due to the nature of the protocols, the size of the file being uploaded is unknown during the transfer. When the transfer chunk is slightly larger than the available quota limits, the file/folder will be created but will leave an empty file or folder (such as zero-byte file).
    - Administrator(s) will be emailed
    - Anti-SPAM email functionality will prevent flooding of admin email accounts
    - For several subsequent attempts to exceed the specified quota, EFT sends notification only for the first one. There are no defined subsequent events that must be triggered for emails to be sent again. However, each failure is logged, audited, and fires events. A successful upload (as a result of increasing quota or just smaller upload that is within the quota limit) breaks the sequence and “resets” the state. The state is in-memory (does not survive re-start) and per-node (is not propagated across HA Cluster). This means if an EFT server service is restarted and the attempts to upload another file after the upload quota has already been reached a new email will be sent. The same is seen when the user connects to a different node that has not sent out an email, EFT will send another email.
    - Message shall be logged at WARNING level with the folder, file name, and user

- Each upload quota failure will log an entry in the eft.log (in a new logger, UPLOAD QUOTA), even if no emails are triggered. For example if the user attempts to upload 10 files after reaching the upload quota, EFT will log those 10 failures.

- The **Activity - Upload Quota Usage** report is available only when adding the System - Report Action to the File Uploaded Event in Event Rules.



Activity – Upload Quota Usage

3/17/2022 16:45:01 Description: This report displays EFT's upload quota usage, monthly, grouped by site name, sub-grouped by the folder.

Month	Limit	Usage
Site: MySite		
Folder: /Usr/F3/		
March-2022	100 MB	0%
Folder: /Usr/q/F3/		
June-2021	100 MB	0%
July-2021	100 MB	0%
August-2021	100 MB	0%
September-2021	100 MB	0%
October-2021	100 MB	0%
November-2021	100 MB	0%
December-2021	100 MB	0%
January-2022	100 MB	95%
February-2022	100 MB	0%
March-2022	100 MB	100%

Viewing Group Membership

EFT creates the following default permission groups for every Site: **Administrators**, **All Users**, and **Guests**. User accounts are assigned to the **All Users**Group automatically. You can create other Groups and add/remove users from Groups. You cannot delete the **All Users** Group.

The procedure below describes how to view which users are assigned to a selected Group.

To view group membership

1. In the administration interface, connect to EFT and click the **Server**tab.
2. Expand the **Groups**nodes, and then click a Group. The **Group Membership** tab appears.
    - The **Member of**box displays the users assigned to the selected Group.
    - The **Not a member of** box displays the users not assigned to the selected Group.

Related Topics

- Creating Permission Groups
- Adding or Removing Users to or from a Group

WTC Users in the VFS

The WTC user folders and files that appear in the VFS are stored:

- On non-HA installations, on the EFT computer (for example, C:\InetPub\EFTRoot\MyGSSite\Usr\).
- On HA installations, in the shared HA configuration location (for example, <shared_drive>\<HA config folder>\InetPub\EFTRoot\MyGSSite\Usr\).

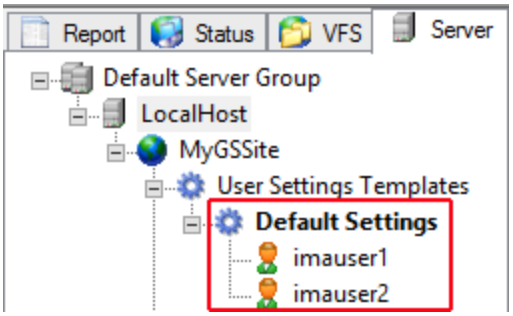
Settings Template Configuration

The topics below provide information regarding creating and managing Settings Templates in the administration interface.

- How Settings Templates Work
- Settings Templates Tabs
- Creating Settings Templates
- Inheritance
- Settings Template Home Folder
- Enabling or Disabling a Settings Template
- Moving a User to a Different Settings Template
- Guest Accounts Settings Template

How Settings Templates Work

Settings Templates exist within a Site and consist of a group of security and access-control settings used as a template. Every client account or user must be a member of a Settings Template. Each new user is assigned to a Settings Template whose settings determine how EFT resources may be used. One Settings Template might be quite restrictive, while another might allow more access to resources. For example, power users would be assigned to a Settings Template allowing greater flexibility in using EFT resources while guest users would be assigned to a more restrictive template where use of EFT resources is very limited. Settings Templates allow an administrator to make changes to the Settings Template that affect all users assigned to that template. The basic profile of individual users can also be changed, overriding the template. Users can also be moved between Settings Templates; users that are moved inherit the properties of the new Settings Template, but retain any modifications (overrides) made by the administrator.



EFT installs with one Settings Template named **Default Settings**. Additional Settings Templates can be added to define access to EFT resources for various types of users. You cannot delete the **Default Template** when it is the only Settings Template.

Settings Templates apply to the Server resources. Use permissions assigned to Groups to control access to folders on your system.

Related Topics

- Creating Settings Templates
- Inheritance

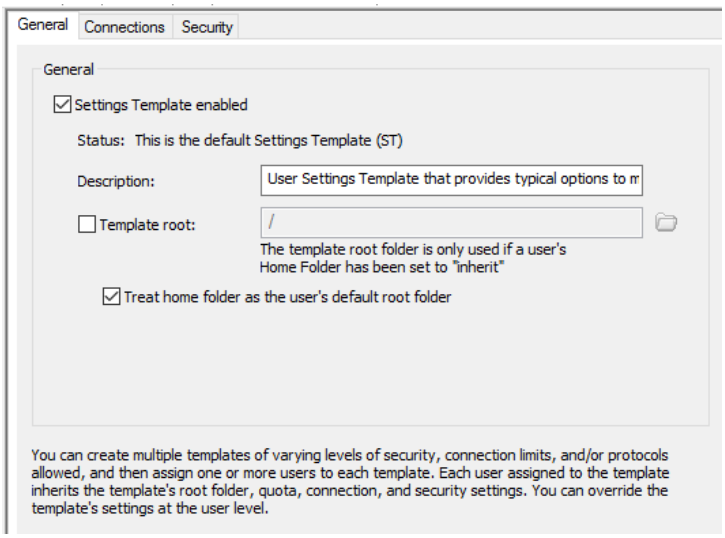
Settings Template Tabs

The **Settings Template** tabs are used to specify connection settings that apply to all user accounts in the Settings Template. Settings on these tabs are inherited by the user accounts; however, you can override these settings in the user account.

- General Tab of a Settings Template
- Connections Tab of a Settings Template
- Security Tab of a Settings Template

General Tab of the Settings Template

The **General** tab of a Settings Template node is used to enable the Settings Template, set the Settings Template as the default, specify the home folder and home folder options, and set a disk quota for each user's home folder. The settings apply to all users assigned to the Settings Template. To apply settings to a specific user, refer to General Tab of a User Node.

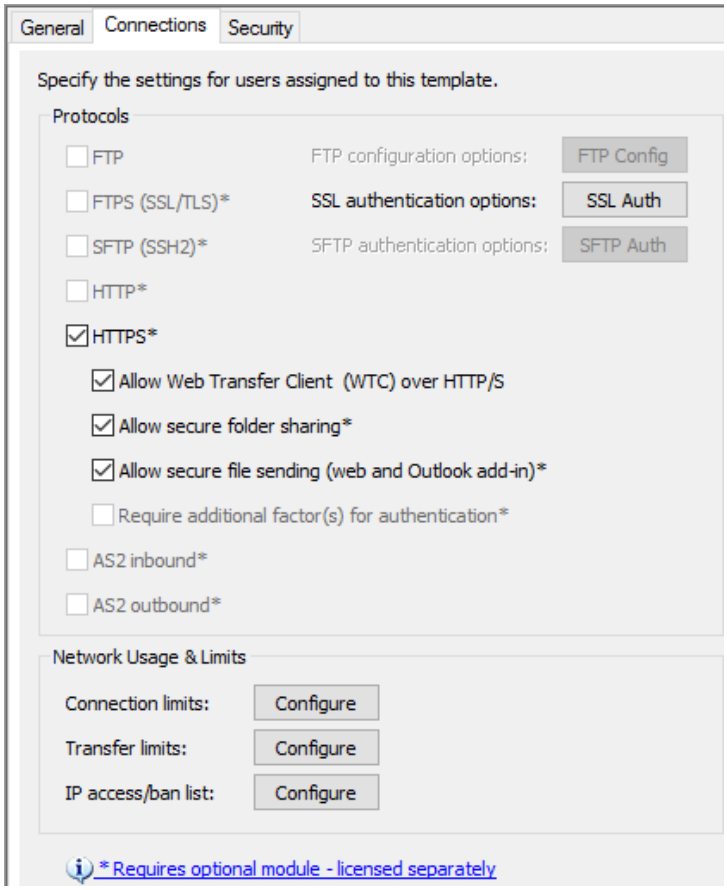


Related Topics

- Enabling or Disabling a Settings Template or User
- Specifying a User's Home Folder
- Configuring User Disk Quotas

Connections Tab of the Settings Template

The **Connections** tab of a Settings Template is used to enable the users in the Settings Template to connect over certain protocols, including using the Web Transfer Client for HTTP/S connections. These settings apply to all user accounts assigned to the selected Settings Template. To apply these settings to a specific user, refer to Connections Tab of a User Node.



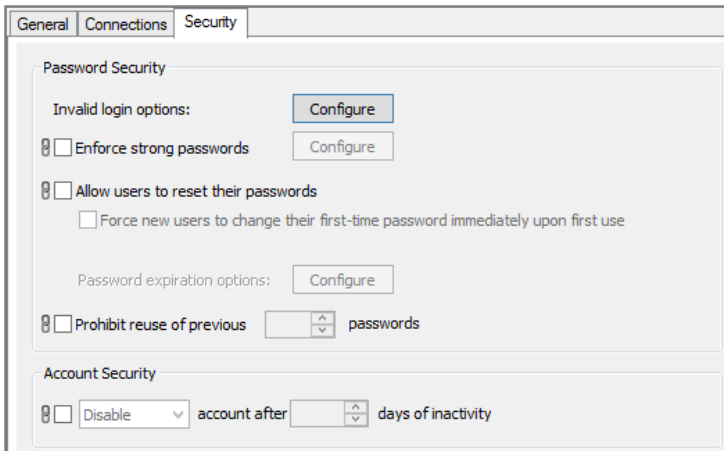
Related Topics

- Listener (Protocol) Settings
- Enabling User Access to the Web Transfer Client
- File Integrity Checking (XCRC)
- Accelerating Transfers with MODE Z
- Allowing or Disallowing the NOOP Command
- Configuring the FTP Connection Banner
- Configuring SFTP Authentication Options for Settings Templates and Users
- SSL Certificate-Based Login

- Configuring AS2 Partners
- Setting Maximum Transfers per Session
- Setting Maximum Transfer Size
- Disconnecting Users on Timeout
- Setting Maximum Transfer Speeds
- Setting Maximum Connections
- Setting Maximum Connections per IP
- Configuring User Disk Quotas

Security Tab of the Settings Template

The **Security** tab is used to specify password and account security settings for all users assigned to the Settings Template. The "link" icons next to the check boxes indicate that the setting is inherited from the Site.



Related Topics

- Disabling or Locking out an Account after Invalid Password Use
- Enforcing Strong (Complex) Passwords
- Expiring Passwords for a User
- Expiring a User Account
- Forcing Password Reset
- Reminding Users when Password is About to Expire
- Password Reuse (History)
- Deleting or Disabling Inactive User Accounts
- Enabling or Disabling a Settings Template

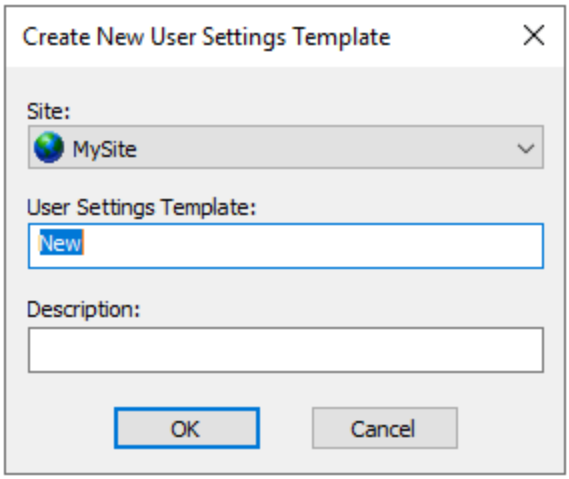
Creating or Deleting Settings Templates

Settings Templates allow you to control EFT's resources while still giving users the flexibility they need to transfer essential files. You can create one or more Settings Templates before or after creating users and assign users to the desired Settings Template. The Settings Template inherits the settings from the Site, but you can override the settings.

To create a new Settings Template

1. In the administration interface, connect to EFT and click the **Server** tab.
2. Do one of the following:
   - Click a Site or any node below the Site, then on the main menu, click **Configuration >New Settings Template**.
   - Click the **Settings Templates** node, then, in the right pane, click **New**.
   - Right-click a Site or any node below the Site, and then click **New Settings Template**.
   - Click a Site or any node below the Site, then press CTRL+L.

   The **Create New Settings Template** dialog box appears.



3. In the **Site** box, click the list to select a Site.
4. In the **User Settings Template** box, type a name for the new Settings Template. For example, type `WTC Users`. The name can contain up to 255 characters.
5. Optionally, type a **Description** for the Settings Template. For example, type: `Web Transfer Client users`.
6. Click **OK**. The new Settings Template appears under the **User Settings Templates** node.
7. Click the new Settings Template, and then click the **General** tab.

8. The Settings Template is enabled by default. To disable it, clear the **Settings Template enabled** check box.
9. If this is to be the default Settings Template, click **Set as default**. (The **Set as default** button only appears on the Settings Template's **General** tab if the template is not the default.) The Settings Template name in the tree will become bold.
10. In the **Description** box, the description you typed in the **Create New Settings Template** dialog box appears. If you did not type a description, you can type one here, but it is optional.
11. If you want to ensure that the Settings Template is not controlling the user's home folder, clear the **STHome folder** check box. Refer to Specifying a User's Home Folder for details about specifying the home folder. This setting affects all users assigned to this Settings Template.
12. If you want to set a disk quota for the users' home folders, select the **Set a disk quota for each user's home folder** check box, then type the limit (in MB) in the **Max disk space** box.
13. Click the **Connections** tab. For information about the settings on this tab, refer to Connections Tab of a Settings Template
14. Click the **Security** tab. For information about the settings on this tab, refer to Security Tab of a Settings Template:
15. Click **Apply** to save the changes on EFT.

To delete a Settings Template

1. Click the template in the list, and then click **Remove**.
2. A confirmation prompt appears. Click **Yes** to remove the Settings Template or **No** to cancel.

Related Topics

- General Tab
- Connections Tab
- Security Tab
- Moving a User to a Different Settings Template
- Inheritance
- The User Tabs

Inheritance

The Settings Template inherits settings from the Site, and a user initially shares the settings of the Settings Template in which the account was created. You can override inherited settings by clearing or selecting the check box. The link icon to the left of the check box indicates whether the setting is inherited from the parent.

Value	Display
Enabled	Check box selected
Disabled	Check box cleared
Inherit from parent; parent enabled	Check box selected with inherit icon
Inherit from parent; parent disabled	Check box cleared with inherit icon
Non-editable, value is enabled	Check box selected but disabled
Non-editable, value is disabled	Check box cleared but disabled

You can change a user's Settings Template by dragging and dropping the user into a different Settings Template, or using the procedure in Moving a User to a Different Settings Template. The account's inherited settings change to reflect the settings of its new Settings Template; however, if a user account contains modified (overridden) settings and is moved to a new Settings Template, those modifications remain in effect at the new Settings Template.

Settings Template Home Folder

You can specify a home folder for the Settings Template, treat the Settings Template's home folder as the user's default root folder, and set a disk quota for each user's home folder in the Settings Template home folder.

To specify the Settings Template home folder

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Settings Template that you want to configure.
3. In the right pane, click the **General** tab.
4. Select the **User home folder** check box, then type the path to the home folder or click the folder icon and browse to the folder.
5. If you want the user's root to be the Settings Template home folder, select the **Treat home folder as the user's default root folder** check box.
6. If you want to specify a disk quota for each user home folder in the Settings Template home folder, select the **Set a disk quota for each user's home folder** check box, then specify a value in MB in the **Max disk space** box.
7. Click **Apply** to save the changes on EFT.

Enabling or Disabling a Settings Template

When you disable a Settings Template, you disable any users in that Settings Template that are not enabled independently of the Settings Template.

To enable or disable a Settings Template

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Settings Template that you want to enable/disable.
3. In the right pane, click the **General** tab.
4. Do one of the following:
    - To disable the Settings Template account, clear the **Settings template enabled** check box.
    - To enable the Settings Template account, select the **Settings template enabled** check box.
5. Click **Apply** to save the changes on EFT. When a template is disabled, a red "X" appears over the template icon .

Related Topics

- Specifying a User's Home Folder
- Setting a User Disk Quota
- Forcibly Logging a User Off EFT

Moving a User to a Different Settings Template

You can move a user to a different Settings Template. For example, if users in the **Default** Settings Template do not have access to the Web Transfer Client, and you want only a select group of users to have access to the Web Transfer Client, you would do the following:

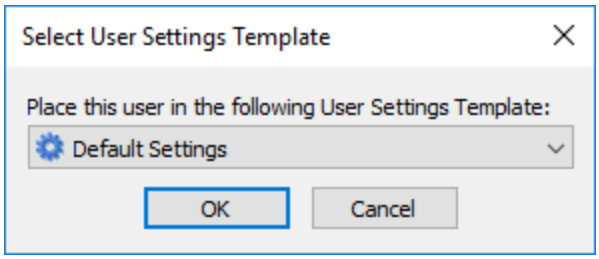
1. Create a new Settings Template and name it "Web Transfer Client."
2. Enable the client for all users in that Settings Template.
3. Move the users from the **Default** Settings Template to the new Web Transfer Client template.

You can move only one user at a time, using drag and drop or the procedure below.

To move a user from one Settings Template to another

1. In the administration interface, connect to EFT and click the **Server** tab.
2. If the new Settings Template is not already created, create the new Settings Template.
3. Expand the node that contains the user you want to move, and then click the user.
4. Do one of the following:
   - On the toolbar, click the **Set Settings Template** icon .
   - On the main menu, click **Configuration >Set Settings Template**.
   - Right-click the user, and then click **Set User Settings Template**.

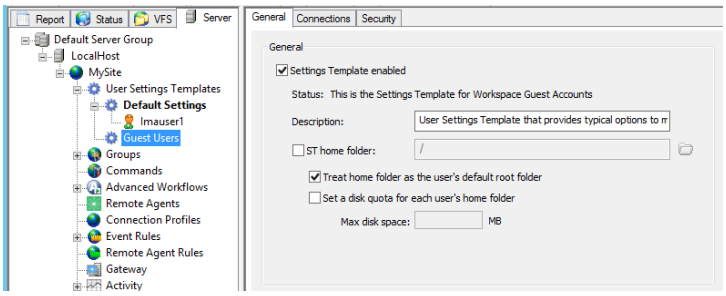
   The **Select User Settings Template** dialog box appears.



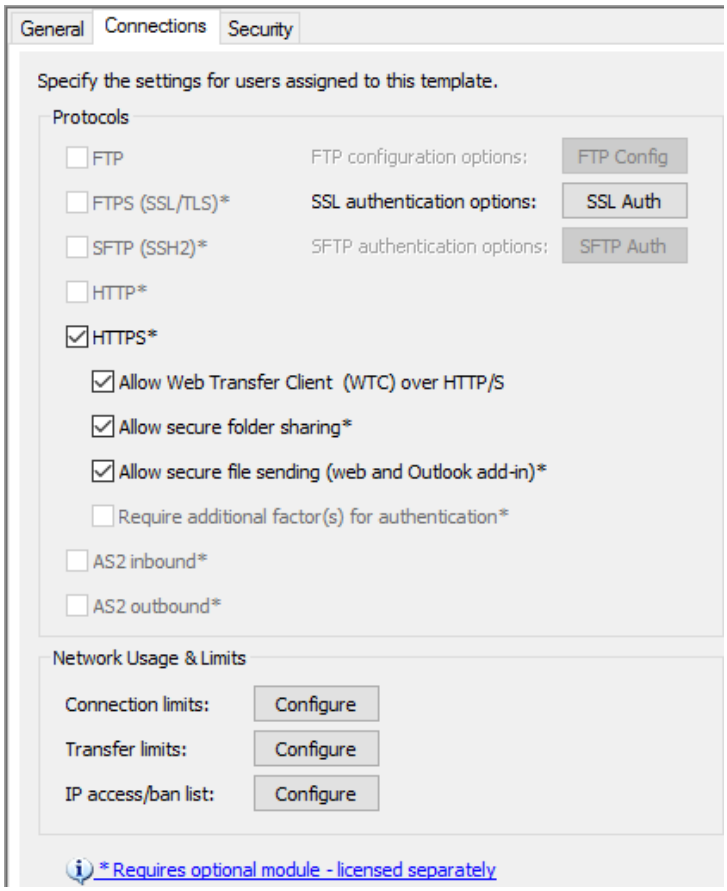
5. Click the list to specify to which Settings Template to move the user account.
6. Click **OK**. The user account moves to the new Settings Template.

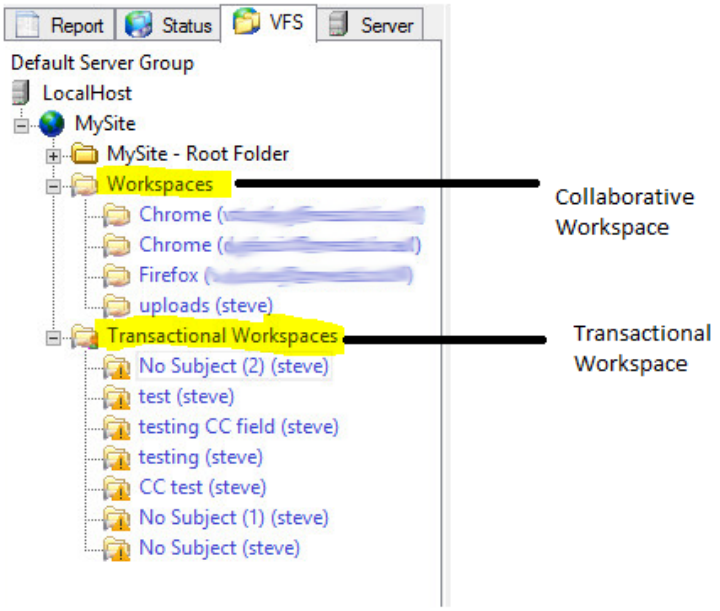
Guest Users Settings Template

After a guest (non-EFT user) has been invitedto join a Workspace, has created an account, and logged in, the guest account will appear (if so configured) in the **Guest Users** Settings template. The **Guest Users** Settings Template appears when Workspaces is enabled. Guest users' permissions depend on what the EFT administrator configures in the **Guest Users**Settings Template. The default settings include **Download**, **Show this folder in parent list**, **Show files and folders in list**. Users with whom a Workspace is shared do NOT have permission to move files and folders out of the Workspace.

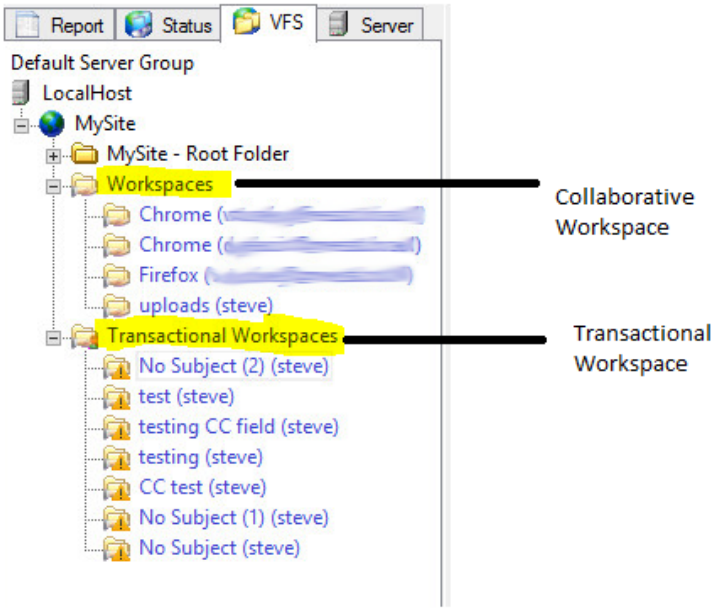


The ability to create Workspaces is disabled by default on the **Guest Users**Settings Template. Disabling creation of Workspaces on **Guest Users** ensures that Workspaces licenses are available for internal users. On the **Connections**tab, you can **Allow Creation of Workspaces** on the **Guest Users** Settings Template for all guest accounts or on each guest account individually. This applies to all guest accounts.





Guest users' folders are created in the VFSin the Transactional Workspaces node of the Site.



Related Topics

- How Settings Templates Work
- Guest Users
- Introduction to Permission Groups
- Sharing Folders (Creating a Workspace)
- Request Files
- Edit-Remove Workspace Permission
- Transactional Workspaces

User Account Configuration

The procedures below provides the instructions for creating, editing, and managing user (client) connections on Sites.

For the procedure for creating an EFT administrator account, refer to Configuring Administrators.

See Password Security Settings for password-related settings that are configured on the Site's **Security** tab for all users.

For information about creating anonymous accounts, refer to Anonymous User Accounts.

- Banning an IP Address that Uses an Invalid Account
- Configuring User Account Details
- User Tabs
- Creating a User Account
- Configuring SSL for a Settings Template or User Account
- Deleting a User Account
- Deleting or Disabling Inactive User Accounts
- Disconnecting Users after a Defined Number of Invalid Commands
- Disconnecting Users on Timeout
- Enabling or Disabling a User Account
- Expiring a User Account
- Forcibly Logging a User Off the Server
- Generating a List of Expired User Accounts and Expiration Dates
- Managing Multiple User Accounts
- Password Security Settings
- Settings Template Configuration
- Specifying a User Disk Quota
- Specifying a Home Folder
- Specifying a User's Permission Group
- Specify GDPR status, Terms of Service, and Privacy Policy Options
- Specifying the Home Folder for AD-Authenticated Users
- Unlocking a User Account
- Updating a User Account's Email Address

- User Account Details Template
- User Login Credentials Message
- Username Resend Message
- Users are Unable to Upload or Download in Home Directory
- Viewing a User's Home Folder
- Viewing User Statistics

Anonymous User Accounts

If you are enforcing strong passwords (defined on the Site or Settings Template **Security** tab), the **Anonymous**options are not available in the **New User Creation** wizard. The option to enforce strong passwords is defined for the Siteor Settings Template, and is then inherited by any Settings Templates in the Site, and then inherited by any users in that Settings Template. Therefore, on a Site with strong passwords enforced and any/all existing Settings Templates inheriting that setting, you would need to either create a new Template (perhaps called "Anonymous Users") with the option disabled, or otherwise create the new user with a temporary password, and then explicitly disable that user's "Enforce strong passwords" option on the user's **Security**tab. With the strong password enforcement disabled for that user, you can click **Change Password** and assign anything you want, including **Anonymous**.

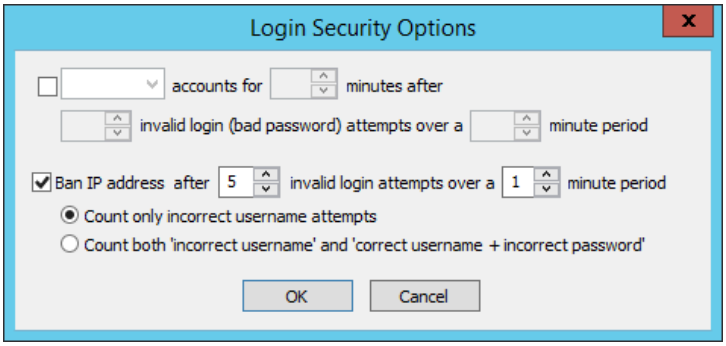
Banning an IP Address that Uses an Invalid Account

EFT can add an IP address to the Site's IP ban list when a specified number of invalid login attempts occur over a specified period when a non-existing username was supplied. The offending IP address is added to the Site's IP address ban list. (The Site's IP address ban list can be viewed and managed on the Site's **Connections**tab.)

EFT **Login Security Options** do not apply to SAML(Web SSO) failed logins. Login security controls, such as password complexity and failed logins, are within the responsibility of the IdP and are not controlled by EFT.

To automatically ban an IP address after a number of invalid login attempts

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site.
3. In the right pane, click the **Security** tab.
4. In the **Password Security** area, next to **Invalid login options**, click **Configure**. The **Login Security Options** dialog box appears.



5. Select the **Ban IP address** check box, then specify the number of invalid login attempts and number of minutes during which to count the invalid logins.
6. Click **OK** to save the changes and close the dialog box.
7. Click **Apply** to save the changes on EFT.

The settings above (6 invalid login attempts over a 5-minute period) cause the IP address to be added to the ban list after the 6th attempt (n+1). The values are the maximum failures ALLOWED before the IP address is banned. After the 6th login failure, the IP address would be banned.

- DMZ Gateway 3.0 and later, EFT communicates the new IP address to the DMZ Gateway, and these attempts are rejected at the edge/DMZ.

- DMZ Gateway 2.0, the IP address is added to the ban list, but the list is not communicated to the DMZ Gateway until the next EFT/DMZ Gateway reconnect.
- If a hacker is using a legitimate username, but is running through a list of passwords, the IP address will be banned, but the legitimate user account is not disabled or locked out. The legitimate user can still login from a valid/non-banned IP address. The IP access/ban list displays newly added IP addresses. (You have to press F5 to refresh to ensure that it displays the current set of IP addresses. The GUI does not refresh automatically.)

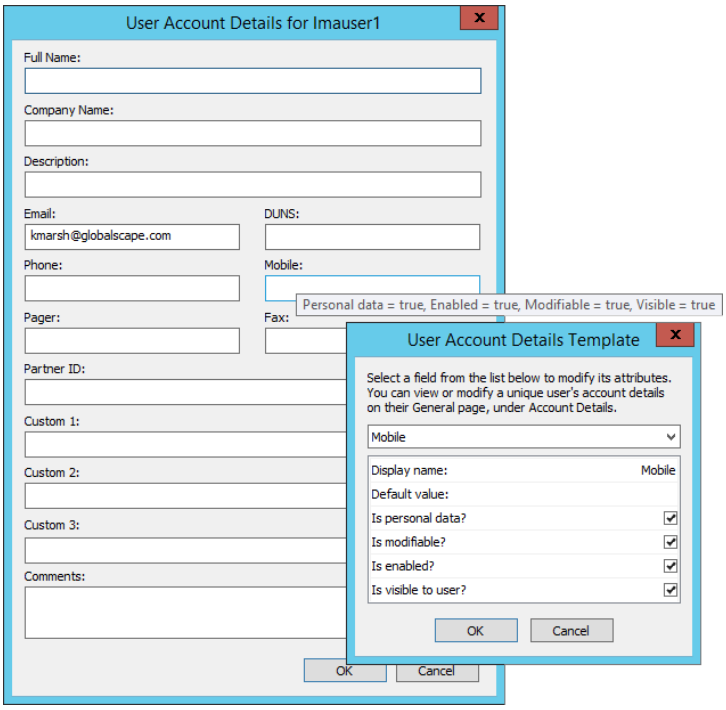
Related Topics

- Disabling or Locking out an Account after Invalid Password Use
- Controlling Access to the Site by IP Address

Configuring User Account Details

The account-specific details associated with a particular user, such as phone number, pager, and email address, are configured on the **Details** tab of a selected user. Some of these fields (such as the email address) can be used in other areas (such as the Event Rules) to notify the user of a completed transaction.

If your organization is required to adhere to privacy regulations such as GDPR, you should specify the settings in the User Account Details Template before continuing. Each field in the **User Account Details** dialog box has a privacy policy assigned to it in the **User Account Details Template** on the **Site > Security** tab. The privacy policy determines whether the administrator can view or change the user account details for a user.



To configure user information

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server** tab, click the user you want to configure.
3. In the right pane, click the Generaltab.
4. Add or change the user's email address in the **email** box on the **General**tab. You can specify multiple email addresses, separated by semicolons. The **email address** box cannot contain more than 255 characters.

5. Click **Account Details**. The **User Account Details for <username>**dialog box appears.
    - The Tool Tips for each box indicate the privacy policy settings from the User Account Details Template.
    - Whether the logged-in administrator is allowed to view or change any of the user account details depends on the settings in the User Account Details Template.
    - The **email**box is populated or updated with what you provide in the **email** box on the **General**tab or the New User wizard; otherwise, it is left blank. If no email address is provided, the User icon in the tree has an information icon on top of it to warn you that the user does not have an email address defined. Accounts should have an email address defined for things like forgotten account information, password reset notifications, expiration, and so on.
6. Complete the user information as needed. All boxes are optional; the **Full Name** and **email** boxes (along with the Server's address book) are used to populate the **Select Names**dialog box in Event Rule email notifications.
7. Click **OK** to close the dialog box.
8. Click **Apply**to save the changes on EFT.

User Accounts

The tabs for a user account are used to specify connection settings that apply only to the selected user account. Settings on these tabs are inherited from the Settings Template, which inherits its settings from the Site; however, you can override these settings on the user tabs.

The procedures below provides the instructions for creating, editing, and managing user (client) connections on Sites.

For the procedure for creating an EFT administrator account, refer to Configuring administrators.

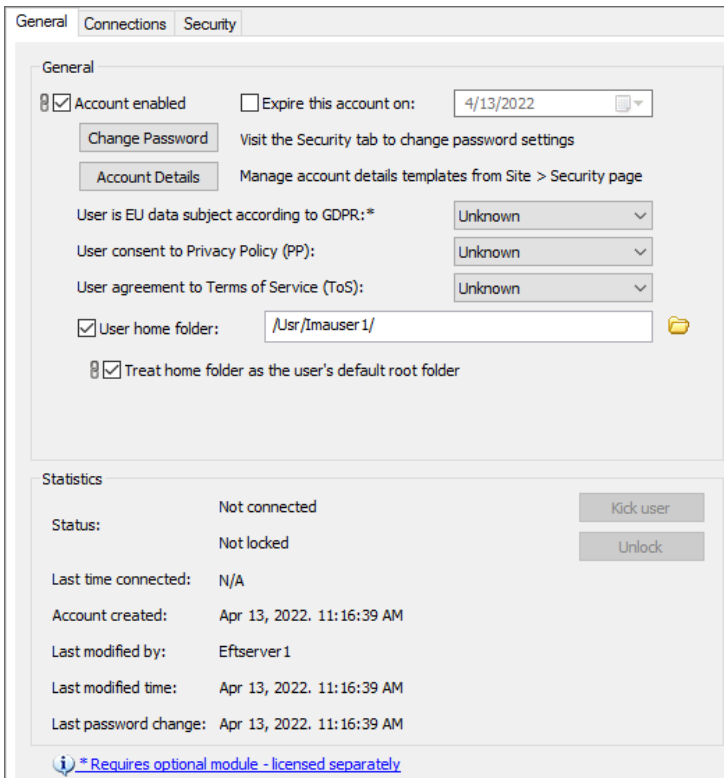
See Password Security Settings for password-related settings that are configured on the Site's **Security** tab for all users.

For information about creating anonymous accounts, refer to Anonymous User Accounts.

- General Tab of a User Account
- Connections Tab of a User Account
- Security Tab of a User Account
- User Icons

General Tab of a User Account

The **General** tab of a user account is used to enable the user account, expire the account on a specific date, specify the home folder and home folder options, set a disk quota for the user's home folder, and viewing the user's statistics. The "link" icons next to the check boxes indicate that the setting is inherited from the Settings Template. The settings apply only to the selected user. To apply the settings to multiple users, refer to General Tab of a Settings Template.



Related Topics

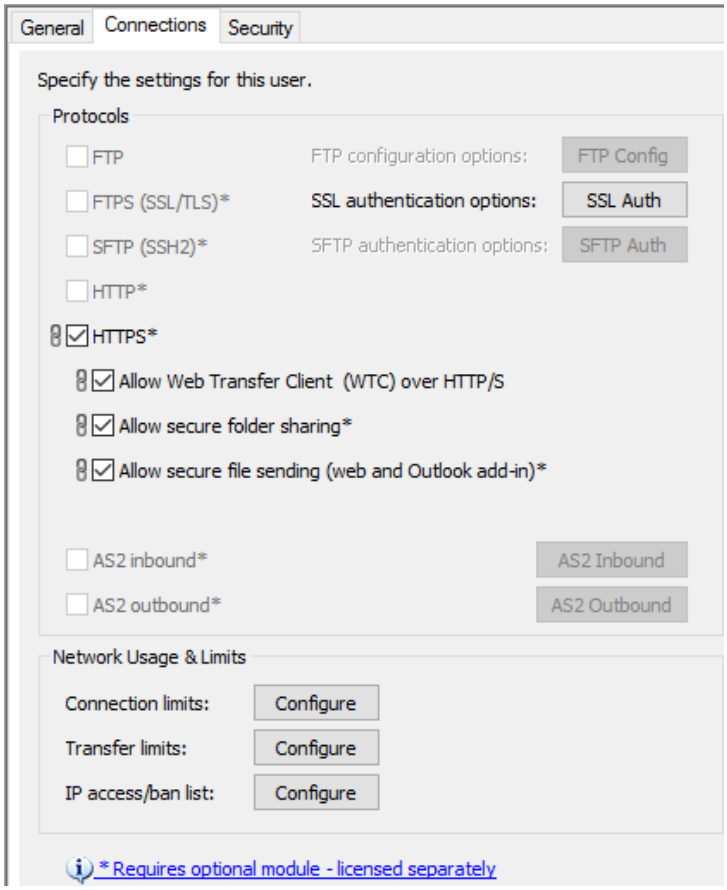
- Enabling or Disabling a User Account
- Expiring a User Account
- Specifying a User's Home Folder
- Configuring User Account Details
- Specify GDPR status, Terms of Service, and Privacy Policy Options
- Changing a User's Password
- Setting the Home Folder for AD-Authenticated Users
- Configuring User Disk Quotas
- Viewing Statistics of a User Account

- Forcibly Logging a User Off EFT
- If Users are Unable to Upload or Download to Home Directory

Connections Tab of a User Account

The **Connections** tab of a user account is used to override the settings in the Settings Template, to connect over certain protocols, including using the Web Transfer Client for HTTP/S connections. You can also configure the user's settings for an AS2 partner account. You can configure the partner manually on this tab or using the AS2 Configuration Wizard.

These settings apply to the selected user. The "link" icons next to the check boxes indicate that the setting is inherited from its Settings Template. The settings that appear dimmed indicate that the setting is disabled in the Settings Template or Site.



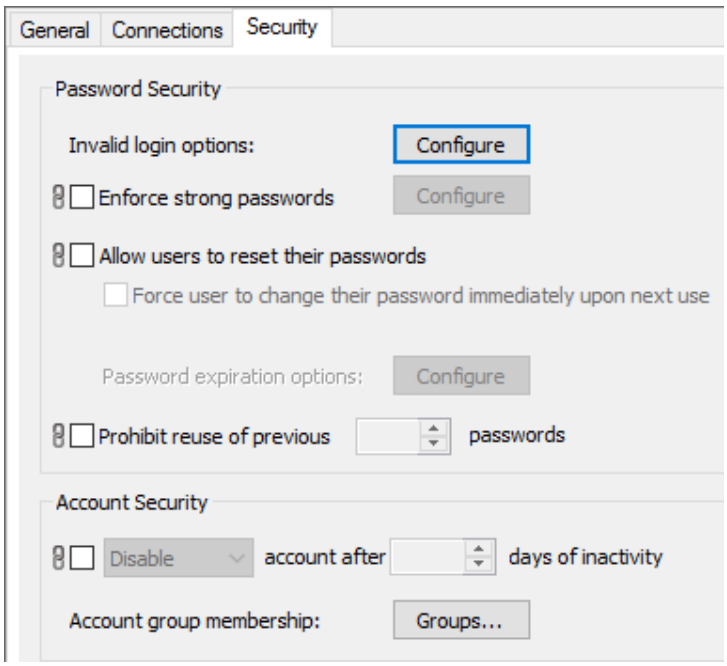
Refer to the topics below for details of this tab.

- Listener (Protocol) Settings
- Enabling User Access to the Web Transfer Client
- File Integrity Checking (XCRC)
- Accelerating Transfers with MODE Z
- Allowing or Disallowing the NOOP Command

- Connection Banner Message
- Configuring SFTP Authentication Options for Settings Templates and Users
- SSL Certificate-Based Login
- Configuring AS2 Partners
- Setting Maximum Transfers per Session
- Setting Maximum Transfer Size
- Disconnecting Users on Timeout
- Setting Maximum Transfer Speeds
- Setting Maximum Connections
- Setting Maximum Connections per IP
- Configuring User Disk Quotas
- WTC & Workspaces - Sharing Files & Folders
- Configuring AS2 Inbound Parameters
- Configuring AS2 Outbound Parameters

Security Tab of a User Account

The **Security** tab for a user account is used to specify password and account security settings and specify the user's Group memberships. These settings apply only to the selected user account. To apply these settings to all users in a Settings Template, refer to Security Tab of a Settings Template. The "link" icons next to the check boxes indicate that the setting is inherited from the Settings Template. The settings that appear dimmed indicate that the setting is disabled in the Settings Template or Site.



Related Topics

- Disabling or Locking out an Account after Invalid Password Use
- Enforcing Complex Passwords
- Allowing or Forcing Password Reset
- Expiring Passwords for a User
- Deleting or Disabling Inactive User Accounts
- Password Reuse (History)
- Removing or Disabling Inactive User Accounts

User Icons

The user accounts defined on a Site are displayed in the **Server pane > Site tree > Settings Template** node, under the assigned Settings Template. The icon displayed for each account provides some indication of the status of the account, as described in the table below.

Icon	Description
	Settings Template without RSA SecurID or RADIUS
	Settings Template with RSA SecurID or RADIUS (small gold key next to blue wheel)
	Enabled user account without RSA SecurID or RADIUS, email address defined
	Enabled user account with RSA SecurID or RADIUS (small gold key next to user icon)
	Enabled user account without RSA SecurID or RADIUS, but missing an email address (blue circle with white letter **i** on top of the user icon)
	Disabled user account with RSA SecurID or RADIUS (small red circle with white x on top of user icon and gray key next to user icon)
	Disabled user account without RSA SecurID or RADIUS (small red circle with white x on top of user icon)
	(RADIUS/RSA requires AAMM.)

Creating a User Account

This procedure provides instructions for creating a user account on Sites that use Globalscape Authentication.

- For the procedure for creating an EFT administrator account, refer to Configuring Server administrators.
- See Password Security Settings for password-related settings that are configured on the Site's Security tab for all users.
- For information about creating anonymous accounts, refer to Anonymous User Accounts.
- An administrator is able to edit account details fields regardless of the modifiable or enabled field attributes set in the User Account Details Template.

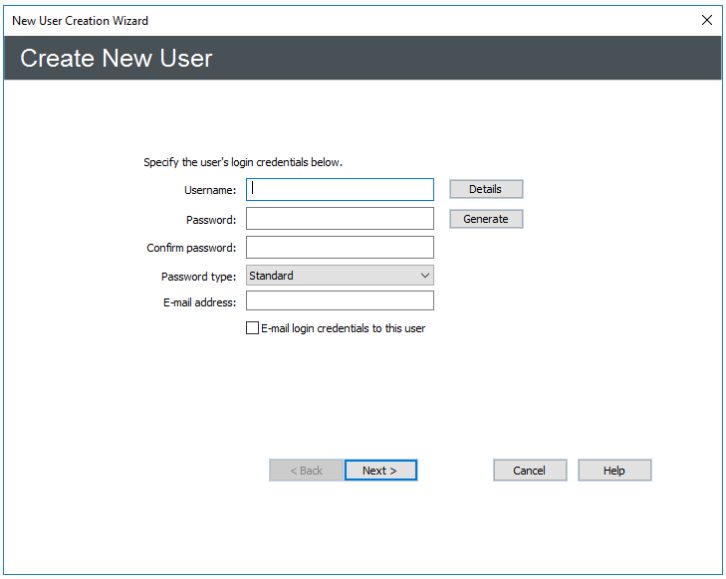
- As of v8.2, the minimum password size is 14 characters.

To create a user account on Globalscape Authenticated Sites

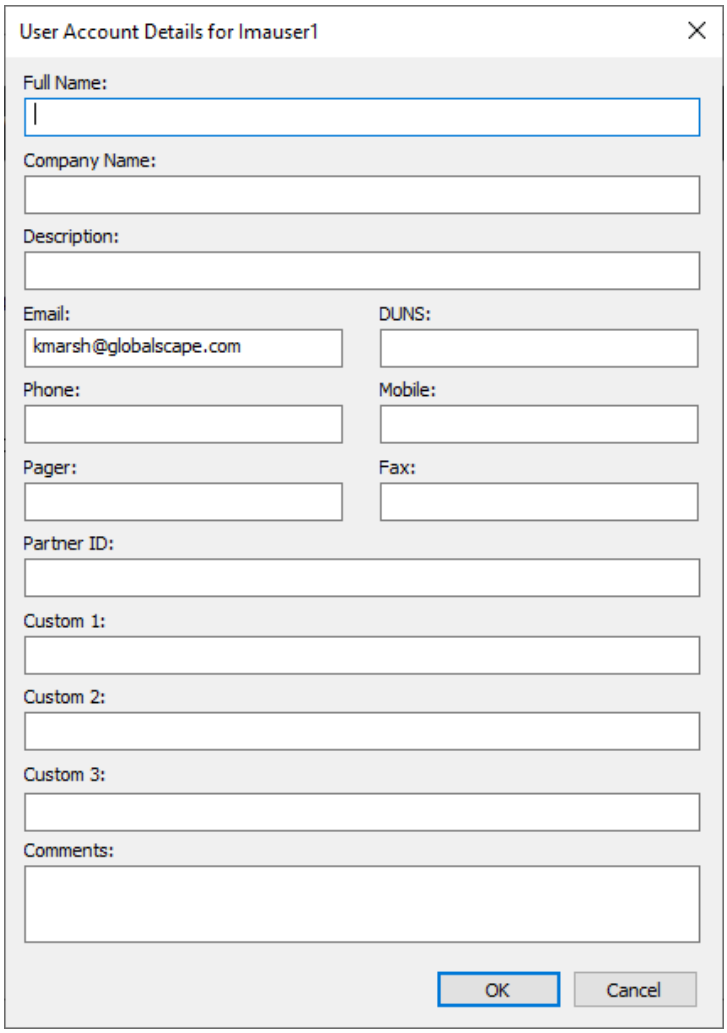
1. After you have completed the Site Setup wizard, you can continue directly to the **New User Creation** wizard. Otherwise, in the EFT administration interface, connect to EFT and click the **Server**tab.
2. Do one of the following:
   - On the main menu, click **Configuration**, then click **New User**.
   - Right-click the **Server**node or any node within it, and then click **New User**.
   - On the toolbar, click the **New user** icon .

   (On Active Directory Sites, if an invalid domain was created, the **New User** option is disabled.)

   The **New User Creation** wizard appears.



3. In the **Username**box, provide the logon name. The following characters are NOT supported:
   `{ } | [ ] \ < > / : ; " ' * + =`
   Username length is limited to 149 characters. (If the path to the user's home folder happens to exceed the maximum number of characters allowed by the Windows operating system, the VFS home folder name will be truncated. The default path is in the Site root `/Usr/%USER.LOGIN%`.)
4. (Optional) Click **Details**. The **New User Account Details** dialog box appears.



a. Provide the user account **Name**, **Description**, **Phone**, **Fax**, **email**, and/or **Pager** information. In the **Custom 1**, **Custom 2**, **Custom 3**, and **Comments** boxes, you can provide other phone numbers, office numbers, mail box number, location, and so on. The **email address** box cannot contain more than 255 characters. You can specify multiple email addresses, separated by semicolons.

> **NOTE:** MFA over SMS can adversely affect Workspaces invitations and ad hoc file send operations when the recipient's phone number is unknown to the sender or Workspace owner. Furthermore, Outlook add-in operations will fail if a recipient doesn't have a phone number associated with the user account.

b. Click **OK**to return to the wizard. (The email address format is validated when you click **OK**. If the email address contains invalid characters or

does not contain the @ symbol, an error message appears. Click **OK**to dismiss the error message, then correct the address.)

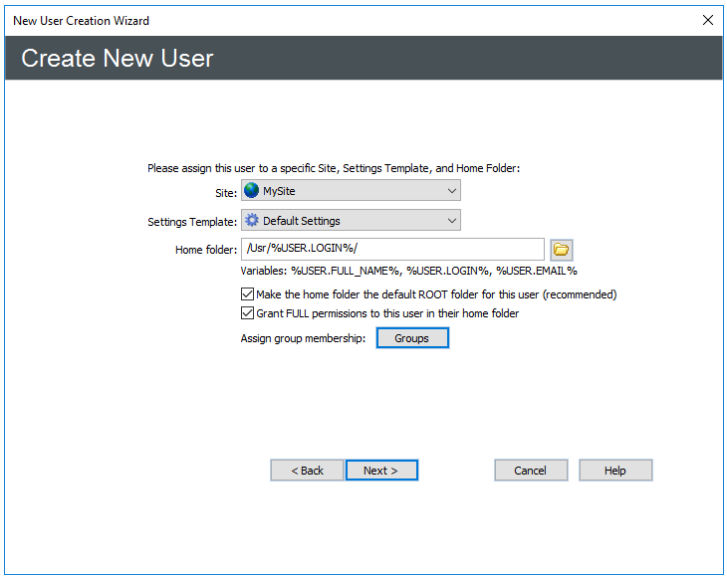
5. In the **Password**and **Confirm password** boxes, provide the account password or click **Generate**to generate a complex password. If you click **Generate**, the password appears in the box so that you can provide it to the user. (If the passwords do not match, an error message appears when you click **Next**.)
6. In the **Password Type** drop-down list, click one of the following:
   - **Standard**- A plain text password is required.
   - **Anonymous**- Any password, including nothing, allows an anonymous connection. (See note below, and Anonymous User Accounts for more information about anonymous passwords.)

     > **NOTE:** PCI DSS requires that you should not use group, shared, or generic accounts and passwords. To address this requirement, EFT hides the **Anonymous**password types for Sites defined using the "strict security settings" anywhere that the password type is selectable.

7. If RADIUS is enabled on the Site (requires AAMM), the Enable RADIUS check box appears under the **Generate**button. The check box is set to inherit the Settings Template/Site setting by default. If the check box is selected, the **Password**, **Confirm password**, **Generate**, **Password type**, and the **email** check box are disabled. If you do not want to enable RADIUS for this account, clear the check box. When the user is created, the account is assigned an auto-generated password based on the password complexity Rules for the assigned Settings Template. Doing so avoids the possibility of a user account with a blank password if RADIUS is disabled.
8. (Optional) In the **email address** box, provide the user's email address. If you do not provide an email address for the user, the user icon is identified as such in the tree, and the account will not be available for multi-user editing. You can specify multiple email addresses, separated by semicolons. The **email address** box cannot contain more than 255 characters. (If you provided an email address in the **New User Account Details**dialog box in step 4 above, the address is copied to this **email address** box.)
9. (Optional) Select the **email login credentials to this user** check box. The username and password are sent to the email address provided. Refer to emailing Users' Login Credentials for details, if necessary.

> **NOTE:** PCI DSS requires that you should communicate password procedures and policies to all users who have access. You can edit the default text of the email that is sent when you create a new user (**CredentialsTemplate.txt)**to include your organization's password policies and procedures. This file is stored in EFT's **Application Data** folder (by default, **C:\ProgramData\Globalscape\EFT Server**).

10. Click **Next**.



11. In the **Site**drop-down list, click the list to select the Site to which you want to add the user. If only one Site is defined, or if you clicked in a Site tree before clicking **New User**, the Site's name is displayed in the list box.
12. Click the **Settings Template** list and click the Settings Template to apply to the new user. All new users are automatically members of the **Default Settings** Template. You can move the user to a different template later if you have not yet defined a custom Settings Template.
13. In the **Home folder** box, type or click the folder icon to browse for and select a path (from the relative Site root) to the user's home folder. The default path is in the Site root `/Usr/%USER.LOGIN%`. You can also add the variables `%USER.FULL_NAME%`and `%USER.EMAIL%`to the path. No verification is performed to determine whether the path is valid.

> **NOTE:** You cannot navigate above the Site root folder.

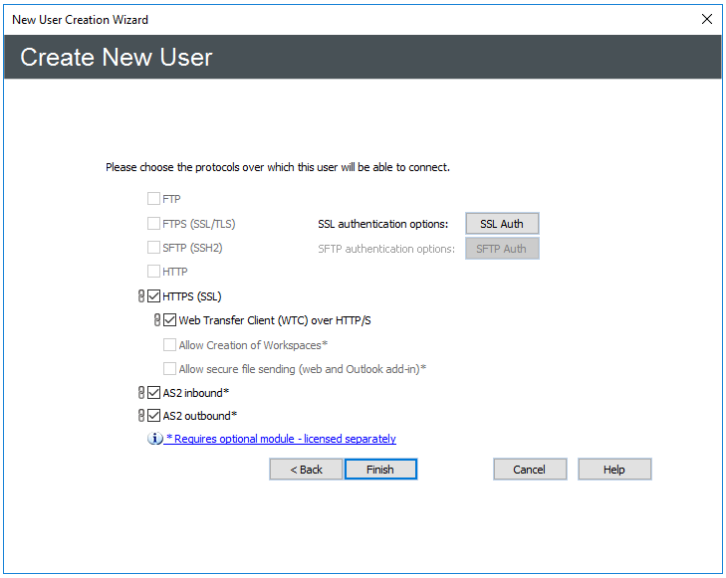
If you use **/Usr/**as the account's home folder (and remove the default %USER.LOGIN%) and clear the **Grant FULL permissions to user in this folder** check box, the account will inherit the permissions of the **/Usr/**folder, which are

Show this folder in parent list and **Show files and folder in list**. The account will not have permission to upload, download, and so on. Refer to Setting VFS Folder Permissions for details of setting permissions on individual accounts.

- The **Make the home folder the default root folder for this user** check box setting is inherited from the User Settings Template/Site, but you can override the setting. If you do not want the user to have a home folder, clear this check box. Select the check box to make the home folder the user's default root folder. Template Settings administrators cannot change this setting when creating a new user. The user inherits the setting from the Settings Template.
- Select the **Grant the user full permissions in their home folder** check box if you want the user to have full permissions to their home folder.

  If you do **not**grant users full permissions to their home folders, they will inherit their Group's permissions.

14. Next to **Assign group membership**, click **Groups**. The **Group Membership** dialog box appears.
15. Permission Groups are used in the Virtual Folder system to assign permissions to users. Each user is assigned to the **All Users** group. To assign the user to one or more other Groups, double-click the Group or click the Group and use the arrows to move the Group between the **Member of** and **Not a member of**boxes, and then click **OK**.
16. Click **Next**. The protocols page appears.



17. Select one or more check boxes next to the protocols on which the user is allowed to connect to EFT. (At least one check box must be selected.) Icons next to the check boxes indicate inherited settings from the Settings Template and Site. Clear the check boxes next to the protocols on which the user is not allowed to connect to EFT. If the text next to the protocol is also appears dimmed, the protocol has not been enabled for the Site and is not available.
    - If you selected any SSL protocol check boxes, click **SSL Auth** to configure SSL authentication options for this user, if different from the Site/Settings Template.
    - If you selected the **SFTP** check box, click **SFTP Auth** to configure SFTP authentication options for this user, if different from the Site/Settings Template. After specifying an SSH key for a user, new user accounts will have the same SSH key preselected.
    - WTC, Workspaces, and secure file sending can be inherited from the Settings Template or specified on the user account.
    - AS2 must be configured on the Site to enable it on the user account. On the user account, You can configure inbound only, outbound only, or both.
18. Click **Finished**.
    - If you selected the AS2 check boxes, a prompt appears regarding configuring this partner's AS2 settings. Click **OK**.

The user account appears in the tree and is selected. To create more users, repeat the procedure above starting with step 2.

Related Topics

- Adding or Removing Users to or from a Group
- Enabling or Disabling a Settings Template or User
- Expiring a User Account

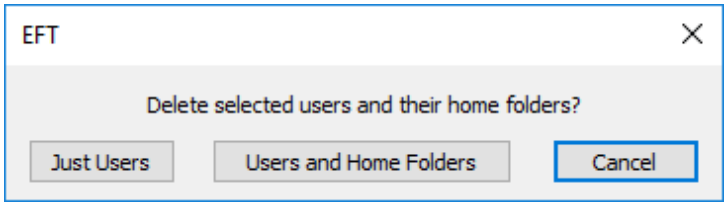
Deleting a User Account

You can temporarily disable a user account, but if the account is no longer needed, you can delete it.

If you remove a logged-on user account from AD, the account is not removed from the interface until after the user logs off and you refresh the interface.

To delete a user account on Sites that use Globalscape authentication

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, under the Settings Template tree, click or right-click the user account, then click **Delete** on the submenu, toolbar, status bar, or keyboard.
3. A confirmation prompt appears asking if you want to delete the selected user(s) and the associated home folder(s). Click one of the following:
    - **Just Users** - Deletes the user account, but keeps the user home folder
    - **Users and Home Folders** - Deletes the account and associated folders. Another prompt appears displaying the path to the home folder for verification. If you want to delete the account and the folder, click **OK**.



    - **Cancel** - Neither the user account nor the home folder is deleted.

Deleting or Disabling Inactive User Accounts

EFT allows you to automatically disable or remove accounts that have been inactive for a period that you specify (1 to 365 days). You can set account security on the Site, Settings Template, and per user. The deletion of accounts is captured in the Auditing and Reporting database for reporting.

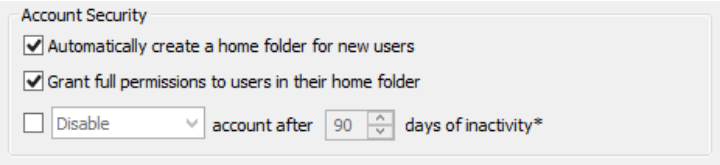
When a high security-enabled Site is created in the Site Setup wizard, the option to delete inactive user and administrator accounts after 90 days is enabled by default. If during Site setup EFT detects that one or more administrator accounts already exist, and that the option to delete administrator accounts after 90 days is not enabled or set to a value greater than 90 days, you are prompted to enable or change that setting.

If a Server administrator attempts to login from a remote system via the administration interface and the password was incorrect or the username does not exist (either because it never existed or because it was removed), when you click **Apply**, EFT does not commit the change, and a warning message appears. In the message that appears, you can accept the non-compliant setting and provide a reason for using this setting (for example, if you are using an alternate solution), or discard the change. If you accept the change and provide a reason, a warning message and the reason that you provided appear in the PCI DSS Compliance report.

- Deleting a user account deletes the account from the authentication manager, but does not delete the user's home folder or its contents.
- EFT executes cleanup procedures every day at 00:00:00 UTC and at Server Startup. This daily server cleanup removes/disables inactive administrators and user accounts and sends password reset and expiration notifications for every Site.
- Any transition from a non-PCI DSS compliant state to a PCI DSS compliant state, or a change in any date-sensitive value, will reset all data value calculations. For example, on a high security-enabled Site, if the administrator disables **Remove inactive administrator accounts after 90 days**, clicks **Apply**, and then immediately decides to re-enable that option, the date values for all administrator accounts are reset from the time the option is enabled, even if the last login dates for those administrators was <n> days ago. The same reset also occurs if you change the password reset period from 30 days to 60 days; that is, the change itself prompts a reset of all the time-based values for that feature.

To specify automatic deletion or disabling of inactive user accounts

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site, Settings Template, or user account that you want to configure, and then click the **Security**tab.



3. In the **Account Security**area, select the **Disable/Remove account after <n> days of inactivity** check box.
4. Click the list to specify **Disable**or **Remove**.
5. Specify the number of days of inactivity after which the account is deleted or disabled. You can specify from 1 to 365 days. 90 days is the default, per PCI DSS 8.5.5.
6. Click **Apply**to save the changes on EFT.

On a high security-enabled Site, if you do any of the following and then click **Apply**, EFT does not commit the change, and a warning message appears.

- Disable the disable/remove inactive account option for administrators or regular users
- Set the inactivity period to a value > 90 days of inactivity
- Change the setting from "remove" to "disable"

In the message that appears, you can discard the change or accept the non-compliant setting and provide a reason for using this setting (for example, if you are using an alternate solution). If you accept the change and provide a reason, the warning and the reason that you provided appear in the PCI DSS Compliance report.

Related Topics

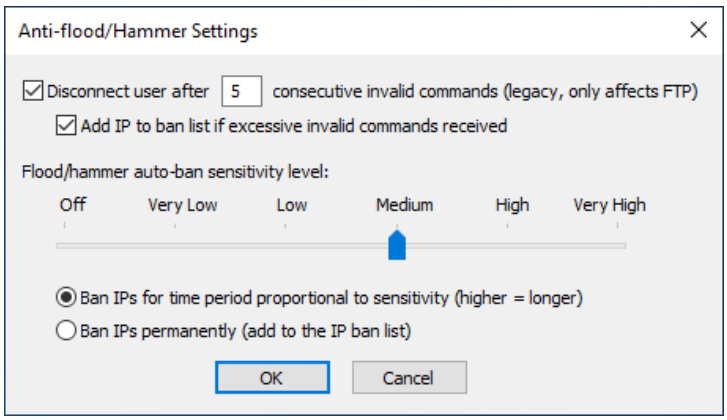
- Automatically Creating a Home Folder for New Users
- Removing Inactive administrator Accounts
- Specifying a User's Permission Group

Disconnecting Users after a Defined Number of Invalid Commands

EFT can automatically disconnect and even ban the IP addresses of users who send an excessive number of invalid commands.

To automatically disconnect users after a defined number of invalid commands

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Connections**tab.
4. In the **Network Usage and Security Settings** area, next to **Denial of Service settings**, click **Configure**. The **Anti-Flood/Hammer Settings**dialog box appears.



5. Select the **Disconnect user after <n> consecutive invalid commands** check box, then type the number of invalid commands allowed before you disconnect the user. You can automatically add the user's IP address to the Site's banned IP address list by selecting the **Add IP address to ban list if excessive invalid commands received**check box. You can later remove the ban on the user by deleting the user's IP address from the list in the Site's **IP Access/Ban List** dialog box.
6. Click **OK** to close the dialog box.
7. Click **Apply**to save the changes on EFT.

See also Flooding and Denial of Service Prevention and Controlling Access to the Site by IP Address.

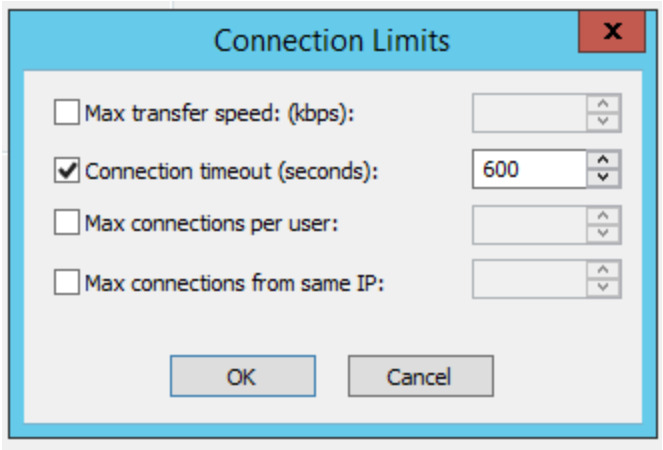
Disconnecting Users on Timeout

You can automatically disconnect users after a specified time of inactivity, set per user or Settings Template. The idle timeout setting applies to FTP, FTPS, and SFTP connections. If a session has been idle for more than the specified timeout, the user has to log back in.

This is different from the Administration Interface Session Timeout and Web Transfer Client timeout values.

To set a maximum idle limit for a user or Settings Template

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the user account or Settings Template that you want to configure.
3. In the right pane, click the **Connections**tab.
4. In the **Connection limits** area, next to **Connection limits**, click **Configure**. The **Connection Limits** dialog box appears.



5. Select the **Connection timeout** check box, then type or select the maximum allowable seconds of inactivity allowed before the user is disconnected.
6. Click **OK** to close the dialog box.
7. Click **Apply**to save the changes on EFT.

Related Topics

- Possible PCI Compliance Report Outcomes
- administration Interface Session Timeout

Enabling or Disabling a User Account

When you disable a user account, the account and user folder are not deleted, allowing you to easily enable or disable the account as needed. (Enabling an account is different from unlocking an account.) When a disabled user is re-enabled in AD, the account is also re-enabled on the AD Site defined in EFT.

To enable or disable a user account

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the user account that you want to enable/disable.
3. In the right pane, click the Generaltab.
4. Do one of the following:
    - To disable the user account, clear the **Account enabled** check box.
    - To enable the user account, select the **Account enabled** check box.
5. Click **Apply** to save the changes on EFT. When an account is disabled, a red "X" appears over the user icon in the left pane .

Related Topics

- If an account has been disabled due to expired Workspaces links, you can configure an Event Rule to re-enable the account automatically when they are sent a Workspaces invitation. Refer to Workspaces Events in the WTC and Workspaces Guide for more information.
- Expiring a User Account
- Unlocking a User Account
- Deleting or Disabling Inactive User Accounts

Expiring a User Account

You can specify a user account to expire on a specific date. Expired accounts are not deleted from EFT; they can be enabled at any time. An expired user account triggers the "User Disabled" Event Rule.

EFT executes cleanup procedures every day at 00:00:00 UTC and at Server Startup. This daily server cleanup removes/disables inactive administrators and user accounts and sends password reset and expiration notifications for every Site. All reminder email messages are sent immediately after flagging the accounts to be reminded.

To disable a user on a specific date (account expiration)

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the user account for which you want to set an expiration date.
3. In the right pane, click the Generaltab.
4. Select the **Expire this account on** check box, and then click the list to select an expiration date.
5. Click **Apply** to save the changes on EFT. On the specified date, a red "X" appears over the user icon on the **Server**tab, and the user account is disabled.

To enable an expired account

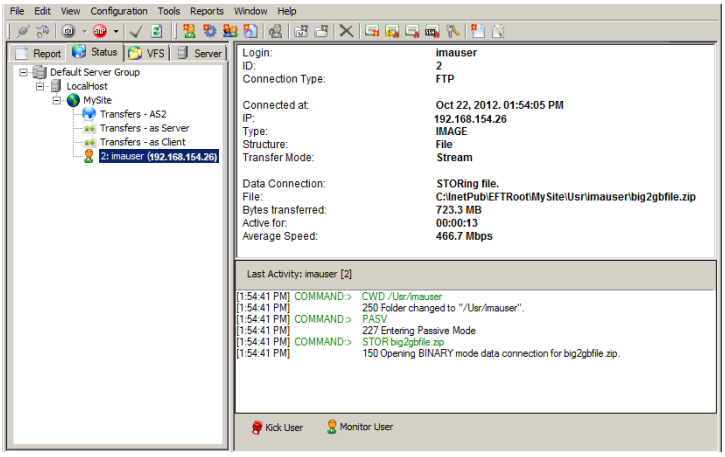
1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the user account that you want to enable.
3. In the right pane, click the Generaltab.
4. Clear the **Expire this account on** check box and select the **Enable this user account** check box.
5. Click **Apply** to save the changes on EFT. The red "X" disappears over the user icon in the left pane.

Forcibly Logging a User Off of EFT (Kick User)

An administrator with Server, Site, or Settings Template permission can manually disconnect a user from EFT in the administration interface. Doing so does not disable users, but only disconnects them from EFT. ("Change Password" administrators do not have permission to kick users.)

To disconnect a user

- In the administration interface, connect to EFT, then do one of the following:
  - On the **Server** tab:
    a. In the left pane, click the user account.
    b. In the right pane, click the **General** tab, and then click **Kick User**.
  - On the **Status** tab:
    a. In the left pane, click the username. The user's statistics appear in the right pane.
    b. At the bottom of the right pane, click **Kick User**.



If the user is connected to the Server using CuteFTP® and has the Smart Keep Alive (SKA) feature enabled, CuteFTP will automatically reconnect to the server. If you do not want the user to reconnect, you must disable the user account on the user's **General** tab (or ask users to turn off SKA).

Generating a List of Expired User Accounts and Expiration Dates

EFT administrators may need to retrieve a list of expired user accounts and view the expiration date of user accounts. This functionality is not yet available in EFT or the Auditing and Reporting module. However, there are commands in the COM interface that can provide this information.

For details of using COM, refer to Globalscape Server COM API. The details of how to get a list of expired accounts is below.

Below is an example for advanced users who can use the example as a guide to creating their own scripts. If you need assistance with creating custom scripts, please contact Globalscape Professional Services.

Determining the Expiration Date for a User Account (GetExpirationDate)

Use the **ICIClientSettings** interface **GetExpirationDate** method to determine the expiration date for a particular user account; set it with **SetExpirationDate**.

Signature:

```
HRESULT GetExpirationdate (
[out] VARIANT *dDate,
[out, retval] VARIANT_BOOL *pVal);
dDate results in a string value, i.e. "4/29/05"
```

Example:

```
Dim strUser: strUser = "test"
set oUserSettings = oSite.GetUserSettings(strUser)
dtAccExpDate =  oUserSettings.GetExpirationDateAsVariant()
WScript.Echo ("dtAccExpDate = "  & dtAccExpDate)
```

In many non-windows environments, "RSmith" and "rsmith" are two different usernames, and case matters. **GetUserSettings** is case **in**sensitive. That is, with this method, "RSmith", "RSMITH", and "rsmith" are all the same user account.

Example Script

The example VB script provided below retrieves user accounts and expiration dates and writes them to a Microsoft Excel spreadsheet. (Of course, Excel must be installed

on the computer on which you are running the script.)

To use the script

1. Copy the script below into a VB script editor.

   In the section that contains EFT address and administrative login, provide your Server address and port and the administrator username and password.

   ```
   'Get Server address and administrative login
      txtServer = "localhost"
      txtPort =  "1100"
      txtUserName = "root"
      txtPassword = "root"
   ```

2. Execute the **.vbs** file.

```
------------------------------------------------------------
START-------------------------------------------------------
' Declare variables
Dim CRLF
Dim EFTServer
Dim Sites, Site, aUsers
'Create the COM Object
Set EFTServer = CreateObject("SFTPCOMInterface.CIServer")
CRLF = (Chr(13)& Chr(10))
'Get Server address and administrative login
   txtServer = "localhost"
   txtPort =  "1100"
   txtUserName = "root"
   txtPassword = "root"
'Connect to Server
On Error Resume Next
EFTServer.Connect txtServer, txtPort, txtUserName, txtPassword
If Err.Number  0 Then
   MsgBox "Error connecting to '" & txtServer & ":" & txtPort &
"' -- " & err.Description & " [" & CStr(err.Number) & "]",
vbInformation, "Error"
   WScript.Quite(255)
End If
set Sites=EFTServer.Sites
'Set Site to first ftp site in list on server
set Site=Sites.Item(0)
Dim objexcel
Set objExcel = createobject("Excel.application")
objexcel.Visible = True
objexcel.Workbooks.add
```

```
arUsers = Site.GetUsers()
 For j = LBound(arUsers) to UBound(arUsers)
        'Name in first column
        objExcel.Cells(j+1, 1).Value = arUsers(j)

        Set oUserSettings = site.GetUserSettings(arUsers(j))
        'boolAccExp = oUserSettings.GetExpirationDate
        dtAccExpDate =  oUserSettings.GetExpirationDateAsVariant
()
        If (dtAccExpDate = "12:00:00 AM") Then
                objexcel.Cells(j+1, 2).Value = "not set to
expire"
                 Else
                objexcel.Cells(j+1, 2).Value = dtAccExpDate
        End If
         objexcel.Columns("A:A").EntireColumn.Autofit
         objexcel.Columns("A:B").EntireColumn.Autofit
 Next

'Close COM connection
EFTServer.Close
' Release interfaces
set oSettings = nothing
set Site = nothing
set Sites = nothing
set EFTServer = nothing
WScript.Quit(0)
----------------------------------------END-----------------------
-----------------------
```

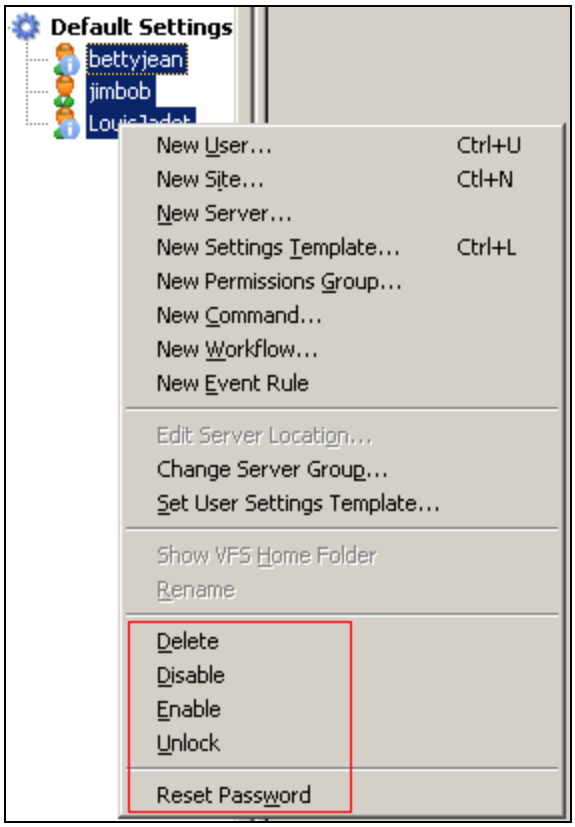
Managing Multiple User Accounts

You can select and manage more than one user account at a time (also known as "batch account management"). For example, you can select multiple accounts and then delete, disable, enable, or unlock the accounts, or reset the passwords on each of the selected accounts.

The selected account must have an email address defined to be able to reset the password.

To select and manage more than one user at a time

1. On the **Server** tab, under the Settings Template tree, press SHIFT or CTRL, and then click each of the users that you want to edit.
2. Right-click the selection, and then click the desired operation, **Delete**, **Disable**, **Enable**, **Unlock**, or **Reset Password**.



Specifying User Disk Quota

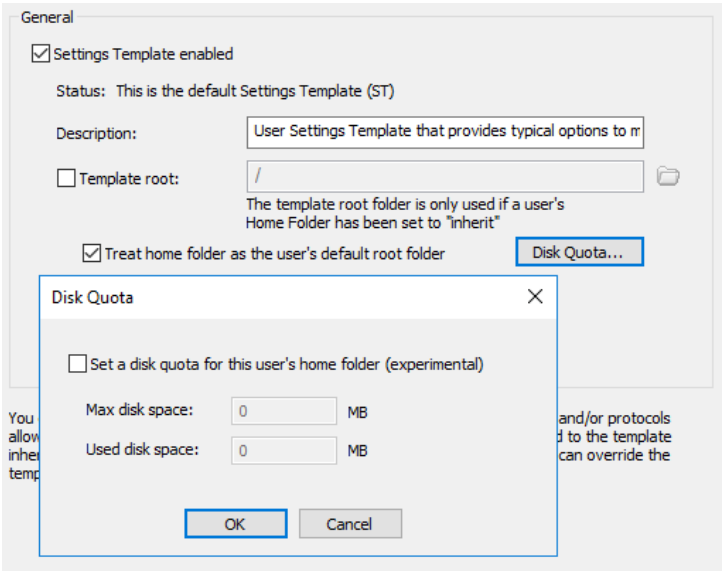
Disk space management is an important aspect of server administration. Setting quotas allows you to specify the maximum amount of disk space available to each user in their home folder.

User quota can set per settings templates or user account and is measured by data on disk. Users do not have a specified disk quota by default.

Upload quota is set at the VFS folder level and is measured based on traffic into the VFS folder, not the size on disk. Upload quotas can be configured at the root level or subfolder, but not both. The upload quota is then inherited to subfolders. Upload quota is specific to the transfers that occur into the server. Additionally, it is not based on a per user transfer and instead collectively captures the quota for the VFS folder via the various protocols.

- You can enable the disk quota options using the advanced property, ShowQuotaControls, described in KB#11429. That is, if you have no need to define a user disk quota, those options are hidden by default.
- Calculation frequency and timeout period can be specified in advanced properties.
- In a cluster, disk quota is specified on each node independently.

When enabled, the **Max disk space** setting on the Settings Template's **General**tab sets the maximum disk space that users can consume in their home folders. EFT administrator can assign a maximum disk space for each user's home folder. Obviously, uploading files increases used disk space and deleting files decreases this number. If the used disk space equals the maximum disk space, the user has to delete files before any more files can be uploaded.



Tip: Create a "User Quota Exceeded" Event Rule to let users know when they need to clean up their files to reduce their used disk space.

An administrator can use Windows File Explorer to add or delete files in a user's home folder, and EFT will update the user's used disk space. Additions and deletions to a user's folder that are performed outside of EFT are ***not***prohibited, even when the total file size exceeds the maximum disk space allowed. However, exceeding the user's used disk space will cause the user to be prohibited from uploading until the used disk space is less than the maximum disk space. This can also occur during parallel uploads from clients like CuteFTP, because EFT evaluates each request independently, not in aggregate, when determining whether the request exceeds the quota limit.

If users report that they are not able to upload files, check whether they have enough disk space available. If not, you or they will need to remove files from their home folder before they can upload any more files with EFT, or you might need to adjust their maximum disk space allowance.

- Disk quota is not calculated upon service start for *all*users with quotas. (This change improves performance during server startup.) Disk quota is calculated on user's login if re-baseline period expired, which becomes the "baseline" disk quota value.
- Upon each upload/download, the user's disk quota value is incremented or decremented.
- The resulting value is stored for that user or template, and it becomes the new baseline at each subsequent login.

- The advanced property DiskQuotaBaselineCalculationFrequencyInDaysallows administrator to specify a re-baseline period in days.
- The administrator can initiate a baseline re-calculation by clicking **Recalculate** on the user account's **General** tab.

To set users' disk quotas

1. Set the properties as shown below in the AdvancedProperties.json file.

   ```
   {
     "ShowQuotaControls": true,
     "DiskQuotaBaselineCalculationFrequencyInDays": true,
     "DiskQuotaBaselineCalculationTimeoutInSec": 20
   }
   ```

   (Ensure there is a comma after the first two properties.)

   In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server** tab, click the Settings Template or user you want to configure.
3. In the right pane, click the **General** tab.
4. Select the **Set a disk quota for this user's default root folder** check box and type the maximum number of megabytes (MB) the user may store in the home folder. The amount of disk quota currently in use appears as a percentage to the right of the **Used disk space**box.

   If you attempt to disable this feature on a high security-enabled Site, a message appears to warn you that this setting violates the PCI DSS, and allows you to continue with reason, or disable the feature.

5. Disk quota is calculated upon user login. Press **Refresh** at any time to view an updated disk quota.
6. Click **Apply**to save the changes on EFT.

Specifying a Home Folder

You can specify the user's login folder at the Settings Template or per user. This is typically set for each user, but the Settings Template can override the user setting.

When you create a Site and select the **Auto assign home folders to newly created users** check box, each user account that is automatically created will have a home folder added as a subfolder of the home folder for the Settings Template to which the user is added. For example, if you add a user "jsmith" to a Settings Template called "Power Users," and that Settings Template's home folder has a path of **/Usr/Power Users/** in the VFS, then this new jsmith account will be generated with a home folder in the Server's VFS of **/Usr/Power Users/jsmith**. This is the default behavior when creating a user within the administration interface. However, you can override/change that behavior when the Site is created. If the user is created using the COM API, or the user appears in the Settings Template as a result of Active Directory, LDAP, or ODBC querying the user account list in real time and finding out that it IS a valid user but not yet added to EFT, then a home folder is added as a subfolder of the home folder for the Settings Template to which the user is added.

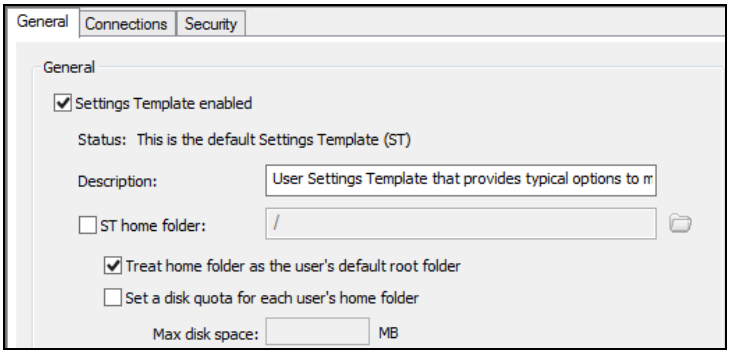
For Sites that use NTLM/AD authentication, if the user account has a Home Folder defined by the AD administrator, then EFT's VFS will **not** create a physical folder for the new user, but instead creates a virtual folder that points to the path specified in Active Directory for the home folder for that user (sometimes called a roaming profile). For example, if jsmith exists on the AD controller as a valid user with a home folder mapped to **\\192.168.20.19\common_file_share\jsmith**, then when jsmith becomes a new user on EFT (using the same path/User Settings Template from the above example), then jsmith will be assigned the home folder **/usr/Power Users/jsmith**, which is a virtual folder pointing to **\\192.168.20.19\common_file_share\jsmith**.

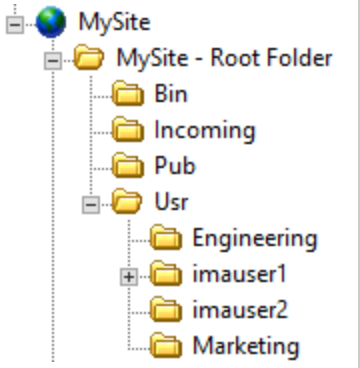
- You cannot specify a physical folder that is outside the Site root for the user's home folder; you must specify a folder under the Site root. You can then create a VFS entry that points to a physical folder outside the Site root. You cannot specify C:\ for the user's home folder.
- **Usr**folders on an HA clustered Siteare stored in the shared configuration path (for example, \\x.x.x.x\inetpub\EFTRoot\mySite\Usr\username).

To view the Settings Template home folder for all user accounts

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the node of the Site you want to configure.
3. Expand the **User Settings Templates** node, then click the Settings Template that you want to view or edit

4. In the right pane, click the **General**tab.





- If the Settings Template home folder is not defined (/), then the user (client) folder (for example, imauser1) is in the root of the Site (for example, /Usr/imauser1)
- If the Settings Template home folder is defined (for example, /Usr/Marketing), then the user (client) folder appears in the Settings Template folder you've defined (/Usr/Marketing/imauser1).

For details of the Virtual File System (VFS), refer to Virtual File System.

To set a specific user's home folder

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server** tab, click the user you want to configure.
3. In the right pane, click the **General**tab.
4. Select the **User home folder** check box. The home folder box becomes editable.

   If you want to ensure that the Settings Template is not controlling the user's home folder, clear the **User home folder**check box in the Settings Template.

5. Specify the path to the user's home folder. You can use variables in the path, such as %USER.FULL_NAME%, %USER.LOGIN%, %USER.EMAIL%.
6. Do one of the following:
   - Type the path to the folder. If you type or paste a path in the **User home folder**box, EFT ***does not*** verify that the folder exists. (Use UNC paths, not mapped drives.)
   - Click the folder icon next to the **User home folder**box. In the **Browse VFS dialog box**, click the folder in which you want the user's folder placed, and then click **OK**.

- Type a forward slash if you want the user's folder to be created at the root of EFT directory instead of the **Usr** directory.

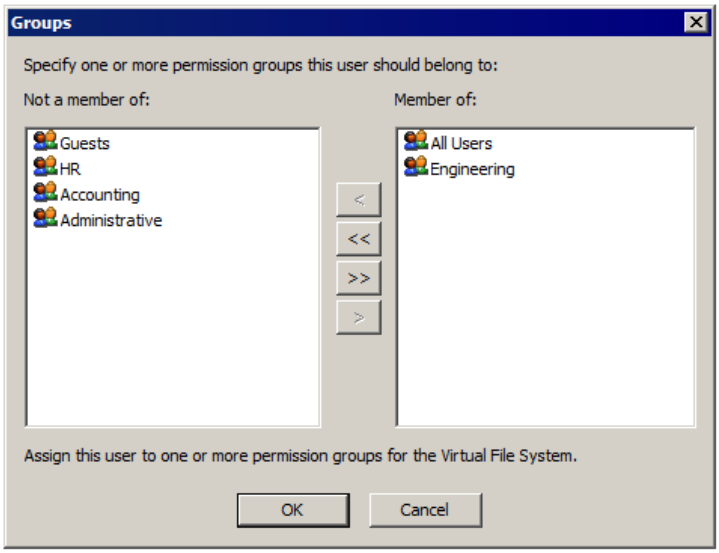
7. Do one of the following:
   - Select the **Treat home folder as default root folder** check box to make the home folder the user's root folder. If the check box is selected, the user cannot browse above their home directory.
   - Clear the **Treat home folder as default root folder** check box. When it is cleared, if you built the Site with the defaults, the user's root folder is **/Usr/<username>**.
8. Click **Apply**to save the changes on EFT.

Specifying a User's Permission Group

When you define a user account, you assign it to one or more *permission*Groups. The Group to which a user belongs determines the user's folder permissions in the Virtual File System (unless you define the user's permissions independent of a Group).

To change a user's Group assignments

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the user that you want to configure.
3. In the right pane, click the Securitytab.
4. In the **Account Security** area, click **Groups**. The **Groups** dialog box appears.



5. To add/remove the user to/from Groups, double-click a Group in the **Member of** or **Not a member** of lists, or click a Group and click the left- or right-facing arrows.
6. Click **Apply**to save the changes on EFT.

Related Topics

- Configuring Groups
- The Virtual File System
- Adding or Removing Users to or from a Group

Specify GDPR Status, Privacy Policy Options, and Terms of Service for Users

The EFT Privacy Policy and web portal Terms of Service agreement can be used to identify or specify whether a user has consented to use of their personal data. This information can help you stay in compliance with GDPR and other privacy regulations. From the Site's **Web**tab, you can configure the agreements, which affect all users on the Site, all web-based portals upon new account registration, anonymous pickup or drop-off, and upon first login. For Site-specific settings, refer to Terms of Service Agreement, Privacy Policy, and GDPR settings.

If consent to use or store personal data is required for use of the service, then you should document WHY the user's consent is required. GDPR Article 7.4 mandates that "utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

Globalscape does not provide the text for your Privacy Policy or Terms of Service agreement. It is up to your organization to create that.

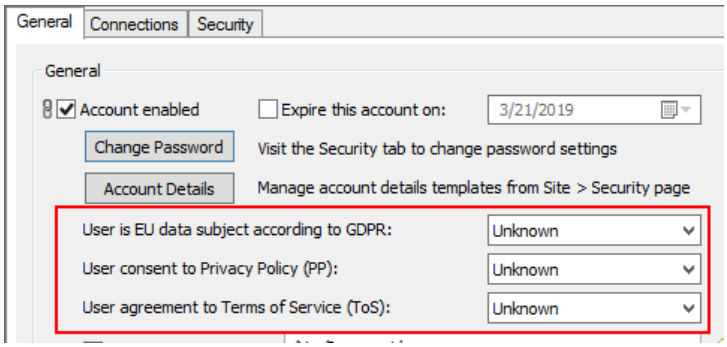
If the Privacy Policy or Terms of Service options are disabled on the **Web**tab, these options are still available on the user account's **General** tab, because the administrator can change them based on agreement or consent from the user, instead of in the browser.

The agreements can be "implicit" or "explicit" agreement:

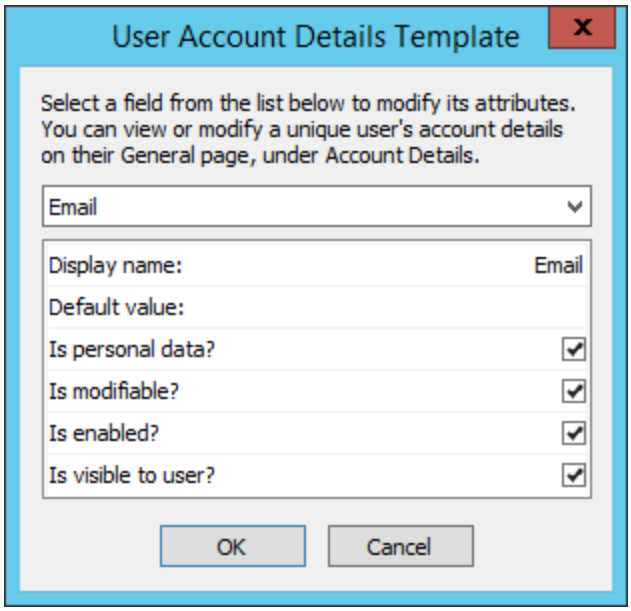
- **implicit** means agreement is implied or understood, e.g., when the user creates an account and provides personal data that is optional for use of the service. (To use EFT, the only required data is an email address and a username/password.)
- **explicit** means agreement is clearly stated, such as in a written agreement that the user account owner has accepted

To specify the user account's options

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the **user account** that you want to configure.
3. In the right pane, click the **General**tab.



4. Under **Account Details**, the **GDPR**, **Privacy**, and **Terms of Service** options appear.
    - **User is EU data subject according to GDPR** - Click **Unknown**, **Yes**, or **No**.
    - For **User consent to Privacy Policy**- Click **Unknown**, **Granted (implicit)**, **Granted (explicit)**, **Denied**, or **Rescinded**.
    - For **User agreement to Terms of Service** - Click **Unknown**, **Agreed (implicit)**, **Agreed (explicit)**, or **Disagreed**, or**Withdrawn**.
5. Click **Account Details**to provide name, company, email, and so on.
6. Go to the **Site**> **Security** tab to specify policies for each field in the **User Account Details Template.**



7. By default, each of the fields have the same policies: **Is personal data**, **Is modifiable**, **Is enabled**, and **Is visible to user**. If you want to change any of those options for any field, select the field in the drop-down, and then clear or select the applicable check box. The attributes in the template apply to all users in all Settings Templates on the Site.

8. Refer to Terms of Service Agreement and Privacy Policy for more configuration, including specifying the actual agreements.

Related Topics

- Logging In (accepting Privacy Policy and Terms of Service)
- Terms of Service Agreement
- User Account Details Template
- Privacy Policy
- GDPR Settings
- GDPR Data Protection Officer
- GDPR-DPIA Report
- GDPR Right Exercised User Events

Specifying the Home Folder for AD-Authenticated Users

By default, the home folder for AD-authenticated users is `/user/%username%`. For some scenarios, you may want to create and assign each AD user a home folder that is actually a Virtual Folder pointing to a specified UNC path. You can do this by editing the user's profile in AD as follows:

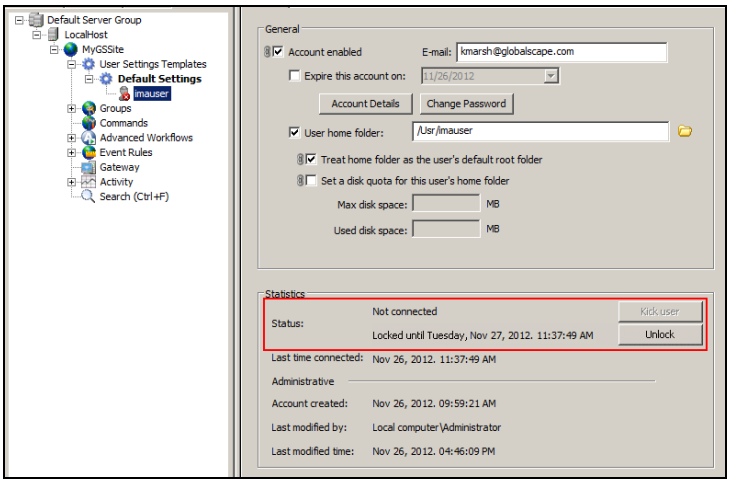
1. Open a user's properties in your AD management tool, click the **Profile** tab, and look at the **Home Folder** section.
2. Click **Connect**, select any appropriate drive letter, then in the **To** box provide the desired UNC path. The UNC path will be used when creating your new AD Authentication site.
3. In EFT, when you create a new AD-authenticated Site, select the **Automatically create and assign home folders to newly created users** check box. If that option is enabled, the Home Folder setting for each AD user's properties will be requested from the network. If that value is set, then a new Virtual Folder will be created in EFT's file system (the VFS) that points to that UNC path. When users log in, they interact with that UNC path that will be treated as their home folder.

   You should enable the option to **Treat home folder as the user's default root folder** on the User Settings Template **General** tab to confine users to their home folder regardless of the NTFS permissions on the directories above, to simplify the client's interface, and facilitate the use of HTTP/S and the Web Transfer Client.

   Due to the lack of standardization among the various LDAP providers, this feature is not currently supported when using LDAP authentication.

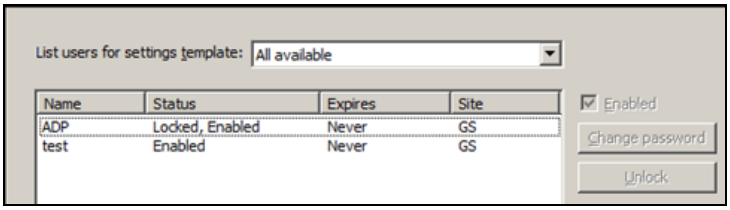
Unlocking a User Account

If a user account is locked out due to invalid password attempts, the user account's user icon in the tree and the user account's **General** tab both indicate that the account is locked. The icon in the tree has a red-circled X on it and the **General** tab's Statistics area indicates the date until which it is locked. (You may have to refresh the interface to see the changes. Also, the view that you see depends on your account permissions.)



- To unlock the user, click **Unlock**.
- You can change the lockout time on the Settings Template's **Security** tab in the **Login Security Options** dialog box.

A sub administrator account would see a view similar to the following illustration:



- In this view, to unlock the user, click the locked user in the list, and then click **Unlock**.

On user accounts that have RADIUS enabled, it is possible for users to lock themselves out of the RADIUS server (for example, due to multiple invalid logins). The user in this case will not be able to log in to EFT, but will not appear to be locked out of EFT in the administration interface. You must unlock the account on the RADIUS server for the user to be able to log in to EFT. For information about unlocking accounts on the RADIUS server, refer to that server's user guide. (Requires AAMM.)

Updating a User Account's Email Address

When the email address associated with an account has changed, you can update it on the account's **General**tab. (The **Email** box in the User Account Detailsdialog box is read-only.)

To update the e-mail address associated with an account

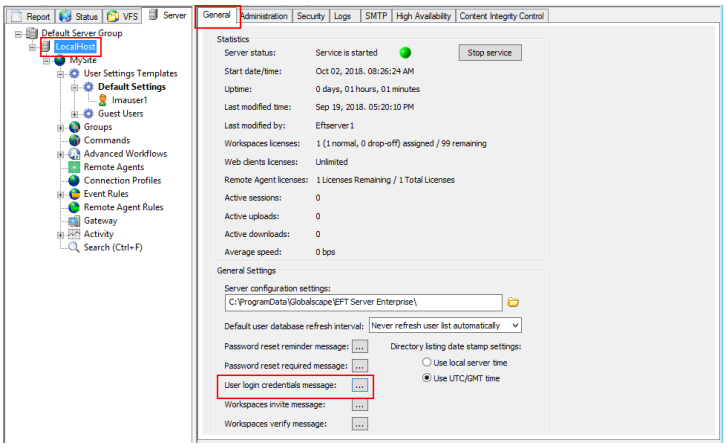
1. On the **Server** tab, click the user account.
2. In the right pane, click the Generaltab.
3. In the **Email**box, provide the new address. You can specify multiple email addresses, separated by semicolons. The **Email address** box cannot contain more than 255 characters.
4. Click **Apply**to save the changes.

User Login Credentials Message

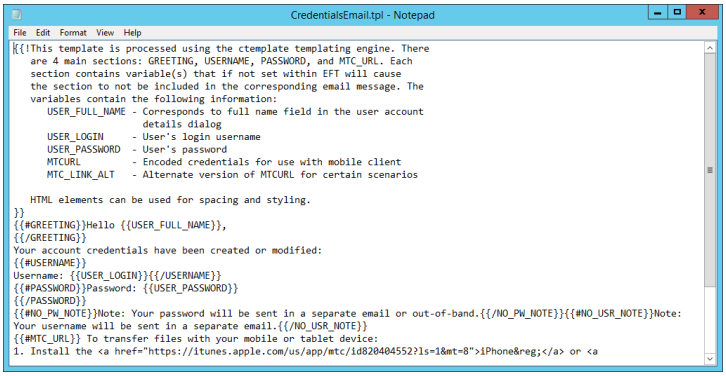
When you create a user, you have the option of sending the user an email that contains the login credentials for connecting to EFT. You can configure the content of the email to apply to all users.

To edit the login credentials reminder

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Server** node.
3. In the right pane, click the **General**tab.



4. Next to **User login credentials message**, click the browse icon . Your default text editor, usually Notepad, opens with the reminder content.



5. Edit the content as needed, being careful not to delete the variables (`%USER.FULL_NAME%`, `%USER.LOGIN%`, `%USER.PASSWORD%`), then save the file and close the editor.

- The file is stored in the **C:\ProgramData\Globalscape\EFT Server\Tempates** directory (by default) and applies to all Sites on the Server.

  To create Site-specific versions

  1. Make a copy of the existing template.
  2. Make your edits (using a text editor, such as Notepad), being careful not edit any of the variables or necessary code.
  3. Save the edited version with the Site name and an underscore prepended to the front of the filename. For example, name it `MyFrenchSite_CredentialsTemplate.tpl`.

6. Click **Apply** to save the changes on EFT.
7. Restart the Site so it can read in the new template.

Related Topics

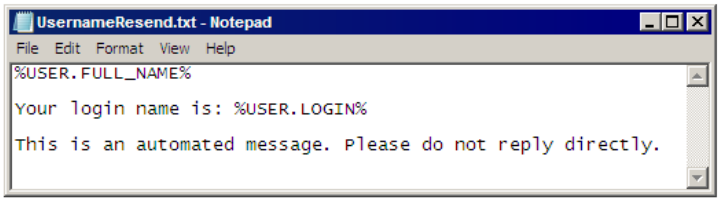
- Username Resend Message
- Password Reset Messages

Username Resend Message

EFT allows users to request their username be resent. You can edit the default message for the Server (which will apply to all users) and for the Sites (which will apply to all users on a Site). The message is an editable text file stored in EFT directory, and accepts EFT variables (for example, `%USER.EMAIL%`), such as those shown in Event Rules.

To edit the username resend message

1. In the **C:\ProgramData\Globalscape\EFT Server\Templates**directory (by default), open the file **UsernameResend.txt**.



2. Edit the text as needed, being careful not to delete the variables (%USER.FULL_NAME%, %USER.LOGIN%), then save the file and close the text editor.
3. Click **Apply** to save the changes on EFT.
4. Restart the Site so it can read in the new template.

Related Topics

- User Login Credentials Message
- Password Reset Messages

Users are Unable to Upload/Download in Home Directory

If users are unable to upload or download files to or from the home directory, first determine whether the problem is just for one or more certain users or all users. If no users can upload or download file, verify that the EFT service has permissions to modify the network share directory. If the problem only occurs for one or more certain users, verify that the user or group has the appropriate permissions in the VFS for that directory.

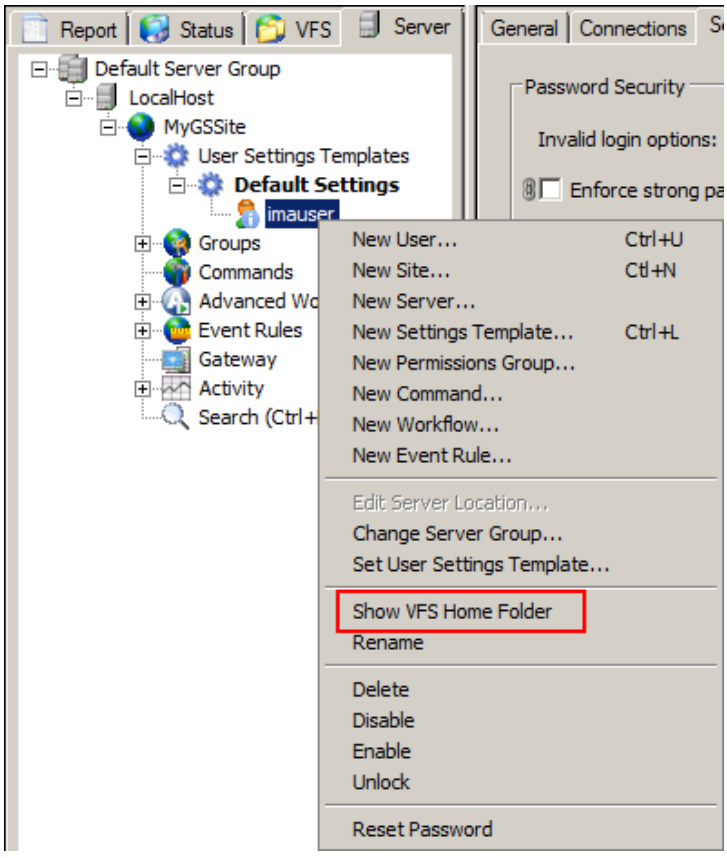
Viewing a User's Home Folder

EFT allows you to specify the maximum amount of disk space available to each user in their home folder on EFT. However, occasionally, you may need to manually manage a user's home folder. In the administration interface, you can right-click a user account to view that user's folder on the **VFS**tab or in Windows File Explorer. For Sites that use Active Directory authentication, also refer to Setting the Home Folder for AD-Authenticated Users.

Virtual folders that point to a drive other than C: or a UNC share are visible using the MLSD FTP command.

To view the user's home folder in the VFS

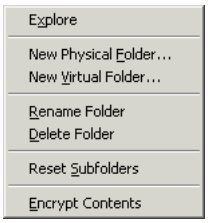
1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server** tab, right-click the user account whose folder you want to view, and then click **Show VFS Home Folder**.



3. The **VFS** tab opens with that user account's home folder selected

To view a user's home folder in Windows File Explorer

1. In the administration interface, connect to EFT and click the **VFS**tab.
2. In the left pane, right-click the user account whose folder you want to view, and then click **Explore**.



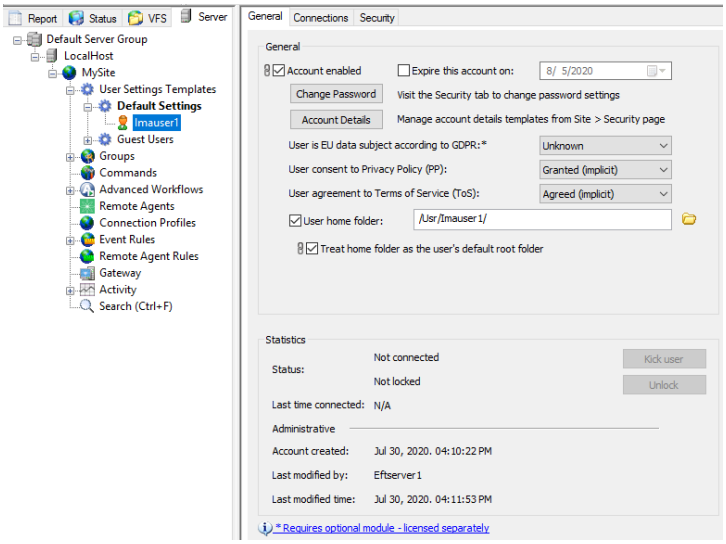
3. Windows File Explorer opens with that user account's home folder selected.

Viewing User Statistics

In the administration interface, you can view the connection status of a user in real time, historical activity, and account administration activities.

To view statistics of a user

1. In the administration interface, connect to EFT and click the **Server** tab.
2. Expand the Site node, User Settings Templates node, and Settings Template node of the user, then click the user that you want to monitor.



3. In the right pane, click the **General**tab. The statistics for the selected user appear in the **Statistics**area.
    - **Status**: Displays "Connected" or "Not connected".
        - Unlock the user by clicking **Unlock**.
        - Forcibly disconnect the user by clicking **Kick User**.
    - **Last time connected**: Displays the date and time that the user last connected to EFT.
    - **Account created**: Displays the date and time that the user account was created.
    - **Last modified by**: Displays the username of the administrator account that created the user account.
    - **Last modified time**: Displays the date and time that the user account was last modified.

Related Topic

- Forcibly Logging a User Off of EFT
- Unlocking a User Account

Password Security Settings

The topics below provide the procedures for configuring the user password rules. (For administrator accounts, please refer to Administrator Account Configuration.

- Emailing Users' Login Credentials
- Changing a User's Password
- Encrypting Passwords
- Enforcing Complex Passwords
- Expiring User Passwords
- AD Password Expiration
- Password Reset Messages
- Allowing or Forcing Password Reset
- Disabling or Locking out an Account after Invalid Password Use
- Prohibiting Password Reuse
- Reminding Users when Password is About to Expire
- Using Login Credentials in Event Rules
- How are Passwords Stored in EFT?

Emailing Users' Login Credentials

When you create a user or change a user's password, EFT can email the login credentials to the user. The option is enabled by default. You can also specify whether to send the username and password in the same email or in separate emails or to only send the username. The email consists of a basic message with dynamic tags for username and password. The email text is defined on Server. Refer to Editing the User Login Credentials Message for details.

To specify email options

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Security** tab.
4. Select the **Enable option to email users their login credentials** check box, then specify one of the email options.
    - email both username and password together
    - email the username and password in separate emails
    - email the username only
5. Click **Apply** to save the changes on EFT.

You can send a password to a user at any time (for example, after you've created the account or changed the password).

To email a user a password

1. In the Change User Password dialog box or the New User Account Setup wizard, type the user's email address, and then select the **Email login credentials**check box.
2. EFT sends the password to the user's email address when you click **OK** in the **Change User Password** dialog box or **Finish**in the **New User Account Setup** wizard.

Related Topics

- Reminding Users when Password is About to Expire
- Editing the Password Reset Messages
- Editing the User Login Credentials Message

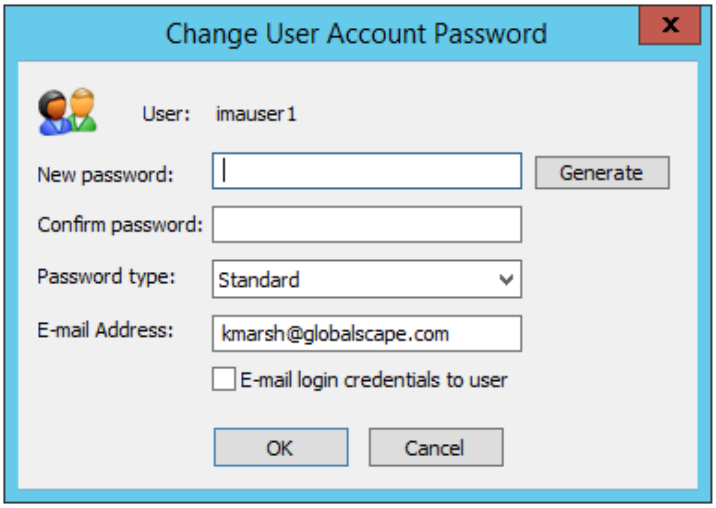
Changing a User's Password

You can change users' passwords from within the administration interface. When a new password is created, EFT determines whether the password meets complexity and reuse requirements.

- The change password function supports user principal and common names (AD/LDAP). That is, it supports UPN (for example, jdoe@globalscape.com; looks like an email address) and CN (for example, jdoe).
- For high security-enabled Sites, you cannot manually create a password; the only option is to click **Generate**to create a unique, complex password.
- If enabled,users can change their passwords in the Web Transfer Client, and the account management web page.
- On AD/LDAP Sites, if you have enabled the "User *must*change password at next logon" feature in AD, you must enable (set to "on") the advanced property described in KB article 10516. If you have enabled the "User *cannot* change password" feature in AD, users will not be able to change their passwords. LDAP over SSL is required to be enabled in order to effectively change your password via WTC.
- If the administrator does not have **Manage personal data** permission, the password appears as dots.
- As of v8.2, the minimum password size is 14 characters.

To change a user's password

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server** tab, click the user you want to configure.
3. In the right pane, click the Generaltab.
4. Click **Change Password**. The **Change User Account Password** dialog box appears.



5. Do one of the following:
   - In the **New password**and **Confirm password** boxes, type and confirm the password. (Not available for high security-enabled Sites.)
   - Click **Generate**. A complex password is generated and entered in the **New password** and **Confirm password**boxes.
6. Click the **Password type** list to specify a type from the following:
   - **Standard**- A plain text password is required.
   - **Anonymous**- Any password, including nothing, allows an anonymous connection.

   PCI DSS requirements state that you should not use group, shared, or generic accounts and passwords. To address this requirement, EFT hides the Anonymous password type for high security-enabled Sites anywhere that the password type is selectable, or if Enforce Strong Passwords is enabled.

7. To email the user's password, type the email address and select the **email login credentials** check box. If the email address is configured in the User Details, the **email Address**box is completed automatically. If you type an invalid email address, an error message appears. (SMTP must be configured on EFT to email the user.)
   - Only administrator accounts with the **Manage Personal Data**permission can see and modify the email address.
8. Click **OK**. The **Change User Account Password**dialog box closes and the email is sent, if configured.
9. Click **Apply**to save the changes on EFT.

Encrypting Passwords

EFT provides the following password-encryption features:

- Two-way TwoFish encryption cipher on passphrases that must be reversible
- One-way hash for passphrases that do not need to be reversible
- Encrypt all passwords used in the following areas:
    - ClientFTP.dll client authentication
    - Authmanager.dll for AD, ODBC, and LDAP authentication
    - PGP private key passphrases
    - ARM connection string password

The PCI DSS states that you should encrypt all passwords during transmission and storage on all system components.

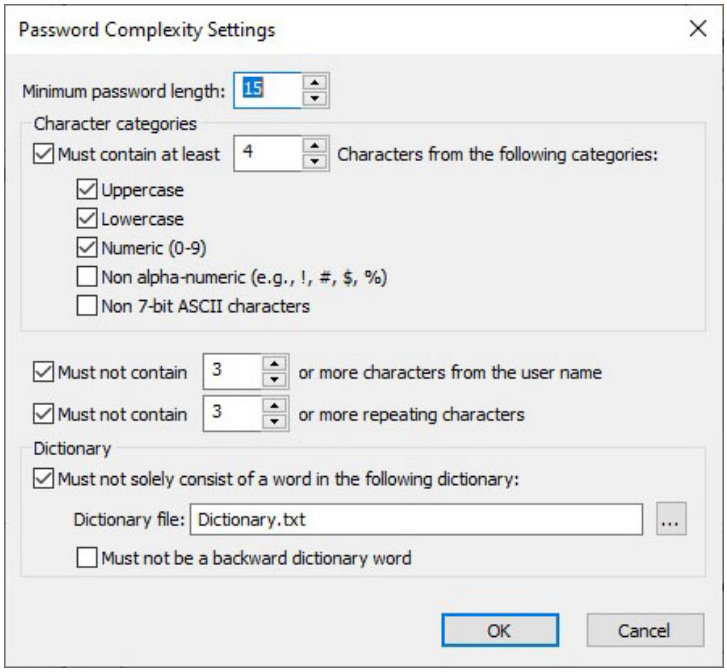
Enforcing Complex Passwords

When you create or update a user account, you can require the user to create strong (complex) passwords. Complex passwords are enabled by default when you create a Site using the "strict security settings" option. (If you also want to create anonymous accounts, refer to Anonymous User Accounts.)

EFT login security controls do not apply to SAML (Web SSO) failed logins. Password complexity and failed logins are within the responsibility of the IdP and are not controlled by EFT.

To require accounts use complex passwords

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site, Settings Template, or user that you want to configure, then click the **Security** tab.
3. Select the **Enforce strong (complex) passwords** check box, and then click **Configure**. The **Password Complexity Settings** dialog box appears.



4. Refer to the guidelines in the table below:

Field	Default	Min/Max Values
Minimum password length - Specify the minimum number of characters that must be in the password	15	6 - 99

Field	Default	Min/Max Values
In the **Character categories** area, if the check box is selected, specify the number and type of characters that must be in the password. • Uppercase • Lowercase • Numeric (0-9) • Non alpha-numeric (for example, !, #, $, %) • Non-4-bit ASCII characters	5	5-99
Must **not** contain N or more characters from the user name	3	2 characters, up to maximum password length
Must **not** contain N or more repeating characters.	3	2 characters, up to maximum password length
Must **not** consist solely of a word in the following Dictionary file. (Click the ellipse icon to select a file.)	on	n/a
Must **not** be a dictionary word backwards (also see note below regarding dictionary words surrounded by special characters)	off	n/a

5. Click **OK** to save the settings or **Cancel**to keep existing settings.
6. Click **Apply**to save the changes to EFT.

For example, suppose you specified that the password must:

- contain at least 6 characters
- contain uppercase letters
- contain lowercase letters
- contain numbers

That means that the password must contain *at least one* uppercase character, *at least one* lowercase character, and *at least one* digit. So in this case, a password could be *A5s3*v35*, but not *a5s3*v35*, because you specified that a password should have at least one uppercase letter.

- The advanced property `{"DictionaryLegacyCheckIncludeSpecialDigits":false}`can be used to strip the special characters from the beginning and end of a password so that EFT can determine if the word is in the dictionary file. For example, the

password "!!Battery9@!" will fail because Battery, a word in the dictionary, is used between the special characters.

- PCI DSS requirements include minimum password lengths, complexity, and reuse rules.
- The dictionary file cannot exceed 10 MB. If you exceed the file size, the Event log will indicate that not all of the file could be loaded. If the dictionary file is not available, EFT operations will continue and a log error is written to the Event log.
- Non-alphanumeric characters are not required by default; you must explicitly specify this option if you want to require it. For those who might be using a non-English language operating system, it is best to leave the **Non alpha-numeric**check box cleared because of characters that are not normally found on a standard keyboard. In this case, your users are free to use non-alphanumeric characters when they create their own password, you just would not require that they do, and the system will not include them when you automatically generate a complex password.
- COM-created accounts are not subject to complexity requirements unless the **CreateComplexPassword**method is used. Refer to the API Reference for details.
- When checking against the user's account name, several characters are treated as delimiters that separate the name into individual tokens: commas, periods, dashes/hyphens, underscores, spaces, pound signs, and tabs. For each token that is three or more characters long, that token is searched for in the password; if it is present, the password change is rejected. For example, the name "Erin M. Hagens" would be split into three tokens: "Erin", "M", and "Hagens". Because the second token is only one character long, it would be ignored. Therefore, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password. All of these checks are case-insensitive.
- **Guest users** - When password complexity is enabled and defined, a guest user's password might fail the complexity test and fail to create the user. In such cases, the user will receive an error message. The guest user should be instructed to create a password that meets complexity requirements defined by the EFT administrator.

Expiring Passwords

EFT provides a method for resetting the password via FTP and SFTP.

Important: Effect of Settings Changes and Template Reassignment on Password Expiration

When modifying password expiration settings or moving a user to a different Settings Template, the password expiration counter may be reset depending on the change applied.

Applying Changes to Password Expiration Settings

If you modify password expiration settings in a Settings Template (for example, changing the number of days before a password expires) and apply those changes to users associated with that template:

- The password expiration counter is recalculated based on the updated policy.
- The system treats the updated policy as newly applied.
- The expiration date is reset and calculated from the time the change is applied, not from the user's original password creation or last reset date.

This means users may receive a new expiration timeline starting from the time the updated policy takes effect.

Moving a User to a Different Settings Template

When a user is moved from one Settings Template to another that has different password expiration settings:

- The password expiration counter is reset.
- The expiration date is recalculated according to the new template's password policy.
- The new expiration period begins at the time the user is assigned to the new template.

Even if the user's password has not changed, reassignment to a new template effectively applies a new password policy baseline.

Administrative Considerations

Administrators should consider the following when updating templates or reassigning users:

- Bulk updates to templates can unintentionally extend or shorten password lifetimes.
- Moving users between templates may delay an upcoming expiration or immediately place a user closer to expiration, depending on the new policy.
- If maintaining the original expiration timeline is required for compliance purposes, plan template changes carefully and communicate with affected users in advance.

To expire a password after <n> days

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server** tab, click the Site, Settings Template, or user that you want to configure, and then click the Securitytab.
3. If **Password expiration options** is not available, select the **Allow users to reset their passwords** check box.
4. Next to **Password expiration options**, click **Configure**. The **Password Expiration** dialog box appears.
5. To expire the password after a certain number of days, select the **Expire passwords in**check box, and then specify the number of days.
6. Do either or both of the following:
    - To send an email when the password is about to expire, select the **Send user an email prior to expiration** check box.
    - To send an email when the password has expired, select the **Send user an email upon expiration**check box.
7. Click **OK** to close the dialog box.
8. Click **Apply**to save the changes on EFT.

If reminders are enabled, users are prompted when their account passwords are about to expire and after the account is expired.

The text of the password expired message, below, is stored by default in **%systemroot%\ProgramData\Globalscape\EFT Server\PasswordResetMsg.html**.

```
%full_name%, The password for account: %username% has
expired. Please change your password at your earliest
convenience. Instructions for changing your password via
```

```
FTP, SFTP, and HTTP/S are provided below for your convenience:
1. Please enter the following URL into your browser: %reset_
page%
2. Supply your current password when prompted
3. Enter your new password and confirm 4.
If approved, exit the browser and login as normal.
```

The text of the password expiration reminder message, below, is stored by default in **%systemroot%\ProgramData\Globalscape\EFT Server\PasswordResetReminderMsg.html**.

%full_name%, The password for account: %username% will expire in %days_left% days. Please change your password at your earliest convenience. Instructions for changing your password via FTP, SFTP, and HTTP/S are provided below for your convenience: 1. Please enter the following URL into your browser: %reset_page% 2. Supply your current password when prompted 3. Enter your new password and confirm 4. If approved, exit the browser and login as normal.

On Sites defined using the "strict security settings," users are forced to change their passwords on first use. Each day it also checks whether passwords are <n> days from expiration, and those passwords are flagged for reminders, if reminders are enabled. All reminder email messages are sent immediately after flagging the accounts to be reminded.

You can enable the password reset page while disallowing general access to HTTP or HTTPS. When a new user logs in to EFT via the HTTP or HTTPS index page, EFT redirects the user to the reset page. After the user creates a new password, they are returned to the index page.

If a user with an expired password logs in over FTP, the user is prompted that the password is expired and must be reset. Until the password is successfully changed, EFT will not process any commands other than changing the password or exiting. If a user with an expired password logs in over SFTP, the user is forced to reset the password before continuing with the login process.

When a password is reset, EFT verifies the new password against complexity criteria and password history, if those features are enabled. Users are not allowed to proceed with their session until a password is created and accepted by the system. If the password is not accepted by the system:

- In HTTPS and SFTP, the authentication request will be denied.
- In FTP, no further FTP commands will be accepted until a new password is provided that meets complexity and password history requirements, if those features are enabled.

- EFT executes cleanup procedures every day at 00:00:00 UTC and at Server Startup. This daily server cleanup removes/disables inactive administrators and user accounts and sends password reset and expiration notifications for every Site. All reminder email messages are sent immediately after flagging the accounts to be reminded.
- There is no way to ask FTP users to change their password prior to logging in. EFT must allow them to login (authenticate), but then prevents any further interaction with their session until they change their password.
- You can edit the HTML file for the password messages; however, be sure not to change the variables, which are enclosed in percent signs (%text%).
- If **Expire password in N days** is enabled, **\manageaccount**and the reset page are enabled, the password has expired, and the user logs in with an expired password, EFT automatically redirects the authenticated user to the reset page. (In HTTPS, the user is redirected to the reset page on the HTTPS port.)
- When resetting passwords, all password complexity requirements, reuse history, and cyclical password-use checks apply, if those settings are enabled in the administration interface.
- **If a Site is running in PCI DSS (high security) mode, warnings will appear when you enable or disable settings that may take you out of compliance.**

Related Topics

- Creating Users
- Expired Password Reminder email
- AD Password Expiration

AD Password Expiration

On AD/LDAP Sites, you can configure EFT through a registry key setting to send an email notifying users that their password is about to expire in <*n*> days. Without this value, EFT (for AD/LDAP Sites) will not attempt to check password status or send notification emails. If the user's password expiration date matches any of the list of days in the registry key, a notification email will be sent to the user's email address specified in the **emailaddress** field of the user's AD account. This default setting sends email notifications 30 days, 15 days, 10 days, 5 days, and 1 day before the password expires. You can edit the number of days and frequency to send notifications.

EFT executes cleanup procedures every day at 00:00:00 UTC and at Server Startup. This daily server cleanup removes/disables inactive administrators and user accounts and sends password reset and expiration notifications for every Site.

The EFT must have "Log On as a domain user" permission for email notifications to work.

For details of advanced properties for passwords on AD/LDAP-authenticated Sites, refer to https://kb.globalscape.com/KnowledgebaseArticle10516.aspx.

Password Reset Messages

EFT provides the option to expire passwords for users. EFT executes cleanup procedures every day at 00:00:00 UTC and at Server Startup. This daily server cleanup removes/disables inactive administrators and user accounts and sends password reset and expiration notifications for every Site.

EFT allows you to set a reminder to notify users of their pending password expiration up to 30 days prior to the password expiration date. You can configure reminder options on the Site, in the Settings Template, and for each user, from 0 (no reminder) to 30 days (5 is the default) before expiration. The reminder can be in the form of a banner message, email, or both.

EFT will send an email informing the user of the pending expiration and provides instructions on how to change the password for one or possibly all protocols if ***all***of the following are true:

- User's password is scheduled to expire
- Email reminder is enabled (The password expiration options are only available if the **Allow users to reset their passwords** check box is selected on the Site's, Settings Template's, or user's **Security**tab. Each will inherit the setting from the parent.)
- User account has an email address associated with it

A user who typically connects over FTP can login via HTTP/S to change the password.

The email reminder messages are editable files stored in the EFT directory, and accept EFT variables (for example, `%days_left%`), such as those shown in Event Rules. You can edit the text of the emails as described in the procedures below.

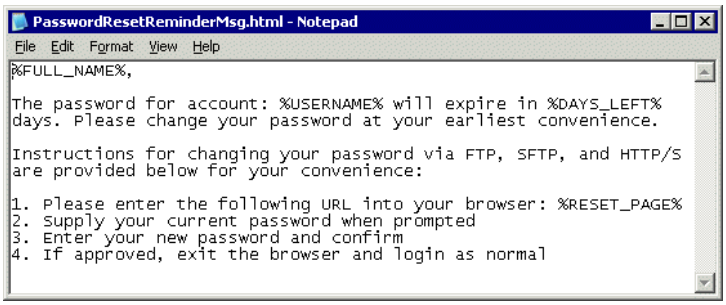
The files are stored in **C:\ProgramData\Globalscape\EFT Server\Templates** directory (by default) and apply to all Sites on the Server. You can also create Site-specific versions (described below).

(In v8.0.5 and later) You can define how long password reset inks should remain valid. The default of 30 minutes is configurable via the advanced property, PasswordResetLinkExpirationPeriodMinutes.

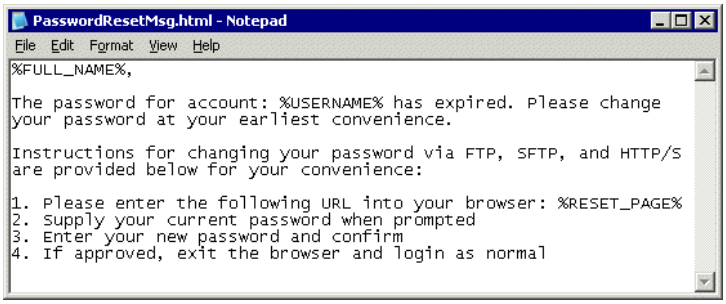
To edit the password reset messages

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Server** node.
3. In the right pane, click the **General**tab.

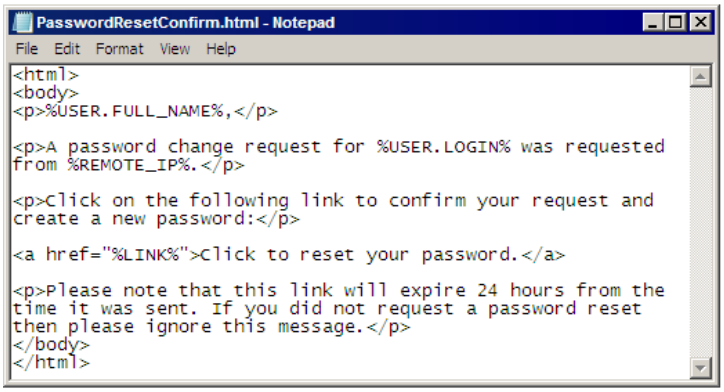
4. Next to **Password reset reminder message**, click the browse icon. Your default text editor (for example, Notepad) opens with the reminder text.



5. Edit the text as needed, being careful not to delete the variables (%FULL_NAME%, %USERNAME%, %DAYS_LEFT%, %RESET_PAGE%), then save the file and close the text editor.
6. Next to **Password reset required message**, click the browse icon . Your default text editor, usually Notepad, opens with the reminder text.



7. Edit the text as needed, being careful not to delete the variables (%FULL_NAME%, %USERNAME%, %RESET_PAGE%), then save the file and close the text editor.
8. To edit the **Password reset confirmation message**, open the file in your default text editor, usually Notepad.



9. Edit the text as needed, being careful not to delete the variables (%USER.FULL_NAME%, %USER.LOGIN%, %REMOTE_IP%, %LINK%), then save the file and close the text editor.
10. Click **Apply** to save the changes on EFT.
11. Restart the Site so it can read in the new template.

To create Site-specific versions

1. Make a copy of the existing template.
2. Make your edits (using a text editor, such as Notepad), being careful not edit any of the variables or necessary code.
3. Save the edited version with the Site name and an underscore prepended to the front if the filename. For example, name it `MyFrenchSite_PasswordResetMsg.html`

Related Topics

- User Login Credentials Message
- Username Resend Message
- Allowing or Forcing Password Reset
- Expiring Passwords
- Reminding Users when Password is About to Expire
- Workspaces Messages

Allowing or Forcing Password Reset

Occasionally, EFT users may want to change their passwords. You may also want them to change their password the first time they log in with the temporary password that you've assigned them. The account management page is provided (via HTTPS) for users to change their passwords without intervention from the system administrator. (You can enable the password reset page while disallowing general access to HTTP or HTTPS, but you still must provide an SSL certificate.)

If **Force users to change their first-time password immediately upon first use** check box is selected, users are forced to change their passwords the first time that they log in to the server. When a new user logs in to EFT via the HTTP or HTTPS index page, EFT redirects the user to the **Change Password** page. After the user creates a new password, they are returned to the home page.

Change password page URL: **https://<EFT Site>/Web/Account/ChangePassword.htm**

- On AD/LDAP Sites, if you have enabled the **User must change password at next logon** feature in AD, you must enable (set to "on") the registry setting described in KB article 10516.
- If you have enabled the **User cannot change password** feature in AD, users will not be able to change their passwords.
- On LDAP Sites, if you have Allowing or Forcing Password Reset, you can also enable the **Suppress "Forgot Password" option** for **All Domains**, **Internal Domain**, or **External Domain**.
- See also the "PasswordResetLinkExpirationPeriodMinutes" advanced property.

When a user logs in to the HTTPS index page for the first time, the user is automatically redirected to the change password page if:

- The Enable account management page over HTTPS check box is selected and the user logs in with a temporary password.
- The Enable account management page over HTTPS and the Redirecting HTTP to HTTPS check box are selected, and the user logs in with a temporary password.
- The user logs in with a temporary password to the FTP port or SFTP engine. (No commands are allowed other than exiting or changing the password until the password has been changed; the user is prompted to change the password.)

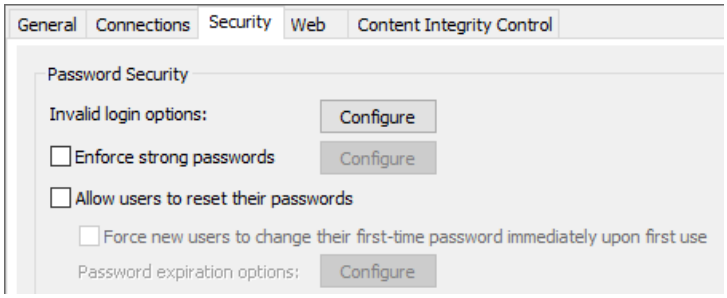
There is no way to ask FTP users to change their password prior to logging in. We must allow them to actually login (authenticate) but then prevent any further interaction with their session until they change their password.

- If an administrator logs in using a temporary password, a warning appears to prompt the administrator to supply a new password. ("Temporary password" means the administrator created a password for them and selected the check box requiring them to change the password when they log in for the first time with that password.)

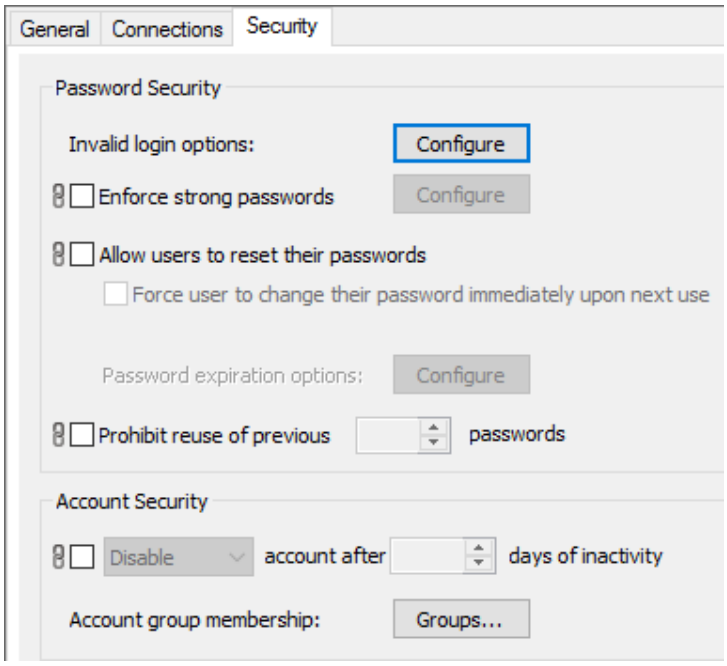
You can configure password reset on the Site, Settings Template, and for each user. (The Site setting **Force new users to change their first-time password immediately upon first use**is inherited by the Settings Templates.)

To configure the Site, Settings Template, or user account to allow or force password reset

1. In the administration interface, click the **Server**tab.
2. On the **Server** tab, click the Site, Settings Template, or User, then click the **Security**tab.
3. Select the **Allow users to reset their passwords** check box.
    - On the Site or Settings Template **Security** tab, to reset their password the first time the user logs in to the server, select the **Force new users to change their first-time password immediately upon first use** check box.



    - On the User's **Security** tab, to reset the password the next time the user logs in to the server (whether they were newly created or of the administrator rest the password), select the **Force user to change their password immediately upon next use** check box.



- To configure password expiration options, click **Configure**.

4. On an LDAP Site, to hide the **Forgot Password** option in the Web Transfer Client, select the **Suppress "Forgot Password" option**check box, then specify whether you want it hidden for **All Domains**, the **Internal Domain**, or the **External Domain**. (Not available on non-LDAP Sites.)
5. Click **Apply**to save the changes on EFT. Users will be prompted to change their password when they log in to the Site.

When a password is reset, EFT verifies the new password against complexity criteria and password history, if those features are enabled. Users are not allowed to proceed with their session until a password is created and accepted by the system. If the password is not accepted by the system:

- In HTTPS and SFTP, the authentication request will be denied.
- In FTP, no further FTP commands will be accepted until the new password is provided and meets complexity and password history requirements, if those features are enabled.

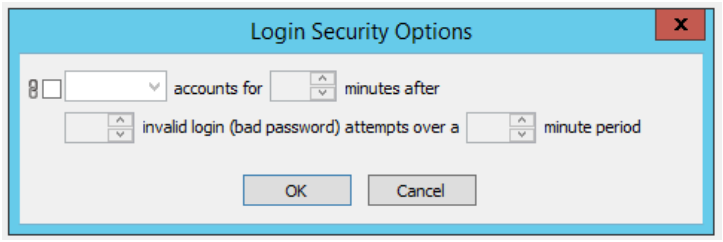
Disabling or Locking Out an Account

EFT can automatically disable or lockout user accounts after a specified number of bad password login attempts over a specified time. This feature can be enabled for a Site, Settings Template, and/or per user. Once an account is disabled, you can re-enable the account on the **General**tab of the user.

- The PCI DSS requires that you should limit repeated access attempts by locking out a user after not more than six attempts and that you should set the lockout duration to thirty minutes or until administrator enables the user account. On a high security-enabled Site, if you clear the **Disable/Lockout**check box or set the maximum login attempts to a value greater than 6, a warning appears.
- EFT **Login Security** options do not apply to SAML(Web SSO) failed logins. Login security controls, such as password complexityand failed logins, are within the responsibility of the IdP and are not controlled by EFT.
- See also Banning an IP Address that Uses an Invalid Account.

Site Login Security Options:

User Login Security Options:



To disable or lockout an account after a defined number of incorrect login attempts

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site, Settings Template, or user that you want to configure.
3. In the right pane, click the **Security** tab.
4. In the **Password Security** area, next to **Invalid login options**, click **Configure**. The **Login Security Options** dialog box appears.
5. Select the check box next to **Lockout**, then specify the following:
    - Whether to **Disable**or **Lockout** the account
    - Number of minutes to lock out the account (30 minutes is the default)
    - Number of invalid login (bad password) attempts after which to disable or lock out the account (6 attempts is the default)
    - Number of minutes during which to count the invalid login attempts (5 minutes is the default)
6. Click **OK** to save the changes and close the dialog box.
7. Click **Apply** to save the changes on EFT.

Related Topic

- Banning an IP Address that Uses an Invalid Account (Site only)

Prohibiting Password Reuse

You can configure EFT to remember a user account's previous passwords and not allow a user to submit a new password that is the same as any of the prior passwords for that account. You can set this at the Site, Settings Template, and user accounts.

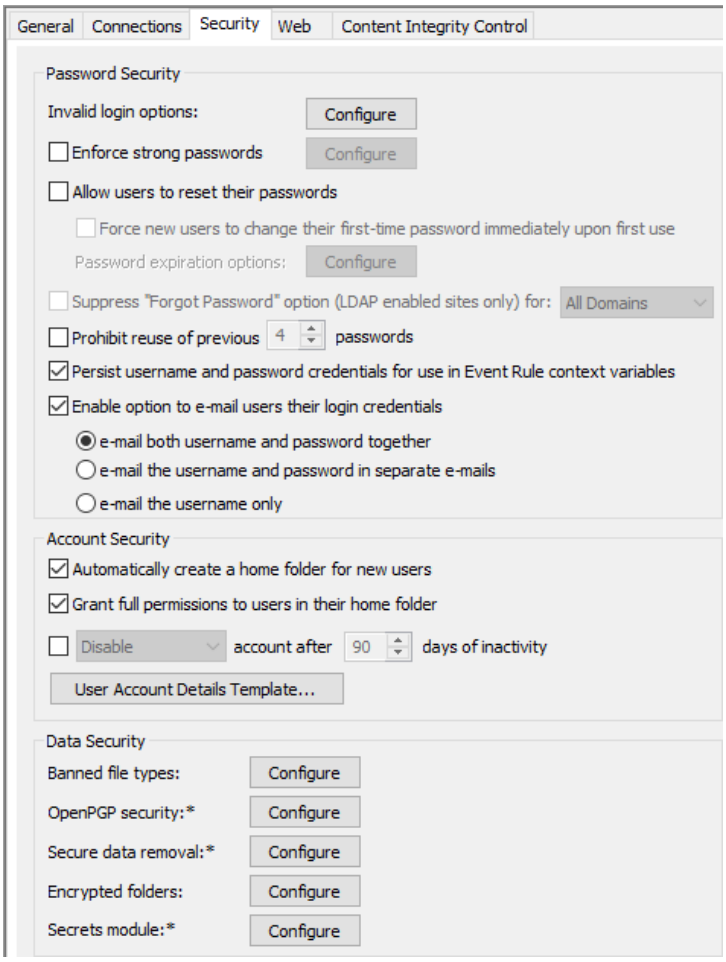
On a high security-enabled Site, password history is enabled by default. If a user attempts to change a password to one of the specified number of passwords previously used for that account, EFT denies the password change request. The option is available at the Site, User Setting, and per user.

EFT validates any password change attempt for reuse (no special casing), whether via COM or the administrator, resulting in a prompt (in the administrator) or an error code (COM).

The password history is reset when transitioning from a non-PCI state to a PCI state. For example, if you disable this option, click **Apply**, then re-enable the option, and then click **Apply**again, the count is started over (the password history is discarded when the option is disabled.)

To enable enforcement of password history

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server** tab, click the Site, Settings Template, or user that you want to configure.
3. In the right pane, click the **Security** tab.
4. Select the **Prohibit reuse of previous** check box, then type the number of passwords to remember.



The number of iterations does not include the current password. For example, if you set password history to 4, and a password change attempt is made, EFT first determines whether the new password matches the current password, then evaluates whether the new password matches any of the previous 4 passwords.

5. Click **Apply**to save the changes on EFT.

Password Reuse Warnings

The following password-reuse violations cause warning messages to appear:

- On a high security-enabled Site, if you disable enforcing password history, a warning message appears.
- If enforcing password history is enabled and a password change request is made by the end-user (either by a user-initiated password reset or a forced reset), and the new password is the same as any of the specified number of previous passwords, EFT rejects the password change attempt. If a password change attempt over HTTP/S fails due to reuse, a warning message appears.

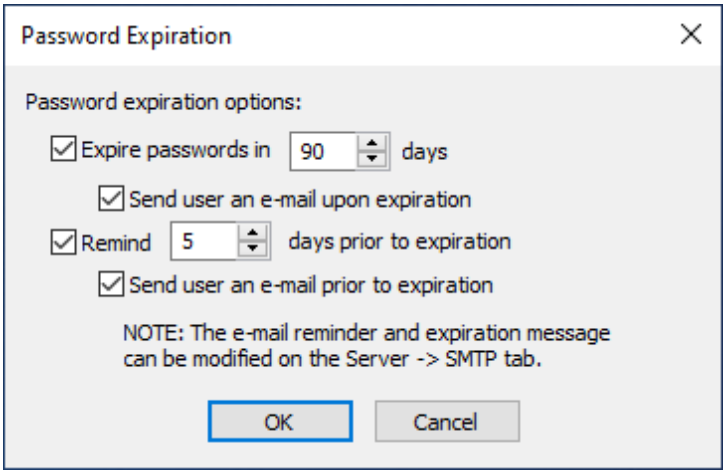
- If a user logged in via FTP attempts to change the login password without being prompted (that is, not a forced reset), and the password fails due to reuse, EFT rejects the password change, but the user may continue the FTP session. If the change attempt was due to a forced reset (that is, require password change on initial login), the user will not be allowed to continue their session until a valid password is provided.
- If a password change attempt over SFTP fails due to reuse, EFT rejects the change and prompts the user to resubmit a valid password. The user is not allowed to continue until a valid password is provided.
- If a password change attempt in the **administrator Login** dialog box fails due to reuse, EFT rejects the change attempt, and a warning message appears.

Reminding Users when Password is About to Expire

EFT allows you to set a reminder to notify users of their pending password expiration up to 30 days prior to the password expiration date. You can set the reminder on the Site for all accounts, on the Settings Template, and/or for each user, from 0 (no reminder) to 30 days (5 is the default). The reminder can be in the form of a banner message or an email or both.

To remind users of expired passwords

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server** tab, click the Site, Settings Template, or user that you want to configure, and then click the **Security**tab.
3. Select the **Allow users to reset their passwords** check box.
4. Next to **Password Expiration Options**, click **Configure**. The **Password Expiration** dialog box appears.



5. Select the **Expire**check box, then specify the number of days after which to expire the password.
6. Select the **Remind** check box, then specify the number of days prior to expiration to remind the user.
7. Do either or both of the following:
   - To send an email when the password is about to expire, select the **Send user an email prior to expiration** check box.

- To send an email when the password has expired, select the **Send user an email upon expiration**check box.

8. Click **OK** to save the settings and close the dialog box.
9. Click **Apply**to save the changes on EFT.
10. Edit the Password Reset Messages, as desired.

    For all protocols, if the user's password is scheduled to expire, the email reminder is enabled, and the user account has an email address associated with it, an email will be sent informing the user of the pending expiration and provides instructions on how to change the password for one or possibly all protocols. A user who typically connects over FTP may optionally login via HTTP/S to change the password.

For details of reusing passwords, refer to Prohibiting Password Reuse.

How are Passwords Stored in EFT?

Refer to the Globalscape Knowledgebase topic #10400 for information about how passwords are stored.

Advanced Authentication Modes Module (AAMM)

The topics in this section provide information about optional security features available in EFT.

- Introduction to the Advanced Authentication Modes Module
- OpenID Configuration
- Common Access Card (CAC) Authentication
- Configuring CAC on an Existing LDAP Site
- Configuring RADIUS Support on an Existing Site
- Configuring RSA SecurID Support on an Existing Site
- Enabling or Disabling RADIUS
- RADIUS for User Authentication
- RSA SecurID Supported Features
- SAML (Web SSO) Authentication

Introduction to the Advanced Authentication Modes Module

The Advanced Authentication Modes Module (AAMM) enables organizations increase adherence to security policies with advanced multifactor authentication features.

The features listed below are activated by the AAMM:

- Common Access Card (CAC) Authentication - EFT has a broader scope of coverage of Common Access Card (CAC) for PIV, which includes support for the PrincipleName or UPN identifier format and the more generalized RFC822Name support. In EFT, CAC is only available on LDAP-authenticated sites.
- RADIUS for User Authentication - Radius allows for integration with third-party solutions, such as SMSPASSCODE for text message verification as a second factor during authentication.
- RSA SecurID - EFT is compatible with RSA's Authentication Manager (AM), version 8.1, for multifactor authentication in conjunction with Globalscape, LDAP, and ODBC-authenticated sites. Globalscape is also an "RSA Secured" partner.
- SAML (Web SSO) Authentication with Just In Time (JIT) provisioning - The HTTP and HTTPS protocols in EFT provide the SAML 2.0 Web SSO profile with HTTP POST binding and corresponding user interface controls for enabling and configuring SAML for achieving Single Sign On (SSO) for Web-based authentication.
- Multifactor authentication via email or SMS for client logins - Multifactor authentication is the process of verifying the identity of a user in which the user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

OpenID Configuration

Instead of asking users to create yet another account and password, you can use OpenID to integrate with an identity provider such as Google or Microsoft that would then redirect the user to EFT. OpenID is an open standard and decentralized authentication protocol promoted by the non-profit OpenID Foundation. It allows users to be authenticated by co-operating sites (known as relying parties, or RP) using a third-party identity provider (IDP) service, eliminating the need for webmasters to provide their own ad hoc login systems, and allowing users to log in to multiple unrelated websites without having to have a separate identity and password for each. Users create accounts on an OpenID identity provider (such as Google or Microsoft), and then use those accounts to sign on to any website that accepts OpenID authentication (such as EFT).

OpenID Connect protocol is supported on ODBC and Globalscape EFT-authenticated Sites. It is configured on the **General** tab of a Site. OpenID works only on HTTPS.

The following OpenID parameters are required to be configured in the OpenID Configuration dialog box:

- **RP Auth path** - Relying Party path to start authentication (client to OpenID Provider)
- **RP callback path** - Relying Party callback to path (client to OpenID Provider)
- **Client ID** - Client Identifier valid at the OpenID Server
- **Client secret** - Client secret which corresponds the "Client ID" at the OpenID Server
- **OP Auth URI** - OpenID provider authentication URI (for Google, it's https://accounts.google.com/o/oauth2/auth)
- **OP Token URI** - OpenID provider token URI (for Google it's https://oauth2.googleapis.com/token)
- **OP x509 Certs URL** - OpenID provider certificate endpoint (for Google it's https://www.googleapis.com/oauth2/v1/certs)

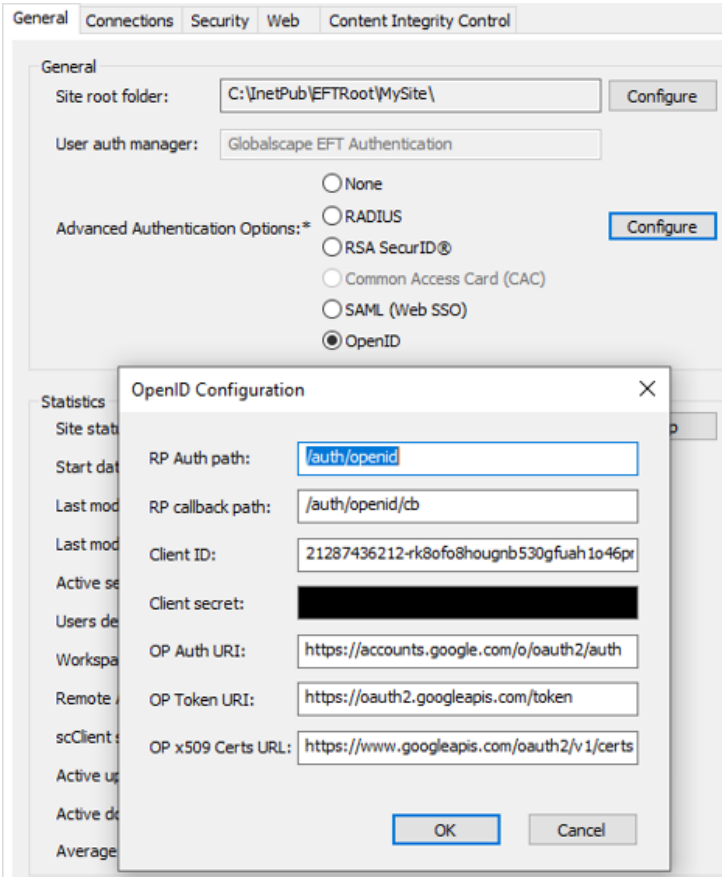
OpenID support requires that the following options be enabled on the Site Connections tab:

- HTTPS should be enabled (OpenID does not work on plaintext HTTP)
- HTTPS Domain field should be configured with a valid domain that will be used to access the authentication URL (e.g., eftserver.com)

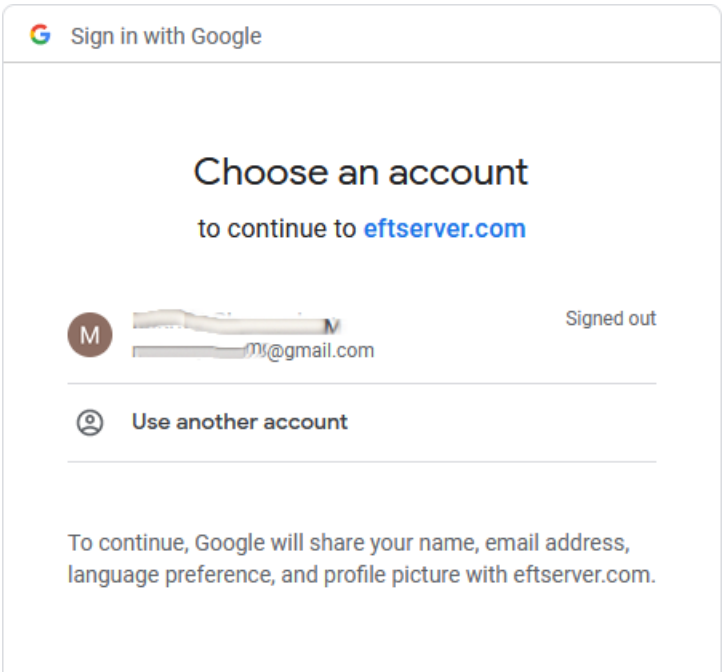
Example of configuring a Google account for OpenID:

1. Set up Google account fo OpenID. Refer to https://developers.google.com/identity/protocols/oauth2/openid-connect for details, including setting up OpenID, obtaining OpenID credentials, setting a redirect URI, and so on.
2. Ensure that all is OK with your Google account using https://openidconnect.net (OpenID Connect Playground).
3. Add to the hosts file (C:\Windows\System32\drivers\etc\hosts) on the EFT computer the line below:
   `127.0.0.1 eftserver.com`
4. Restart Windows.
5. In the EFT administration interface on the **Site > Connections** tab, select the **HTTPS** check box and set the **Domain** field to eftserver.com.

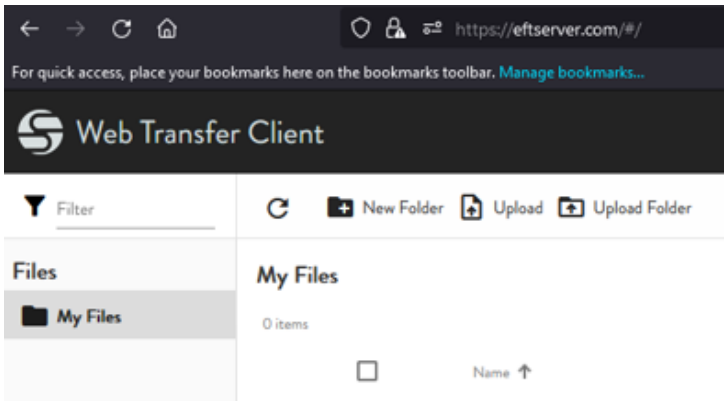
6. On the **Site > General** tab, next to **Advanced Authentication Options**, click **OpenID**, then click **Configure**. The **OpenID Configuration** dialog box appears.



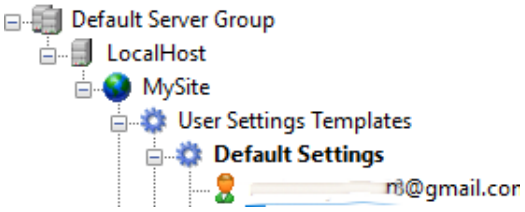
7. Open a browser window and in the browser's address box, type `https://eftserver.com/auth/openid` then press ENTER.



8. Select your account and login. The WebTransfer Client appears.



9. In the EFT administration interface, a new user with your email address appears.



OpenID login< > EFT workflow goes like this:

1. Set up Google account (for example).
   (Refer to https://developers.google.com/identity/protocols/oauth2/openid-connect)
2. The browser redirects by EFT to <OP Auth URI> with necessary parameters.
   (For Google, it's https://accounts.google.com/o/oauth2/auth.)
3. The client logs in to the OpenID Provider.
4. The OpenID Provider redirects back to EFT.

   The client is added to EFT as a new user and is logged in.

RSA SecurID Supported Features

(Included in Advanced Authentication Modes Module) EFT can be configured to communicate with RSA Authentication Manager via native SecurID protocol or RADIUS protocol.

Feature	Supported?
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	Yes
On-Demand Authentication via API	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of administrative Interface	No

Related Topics

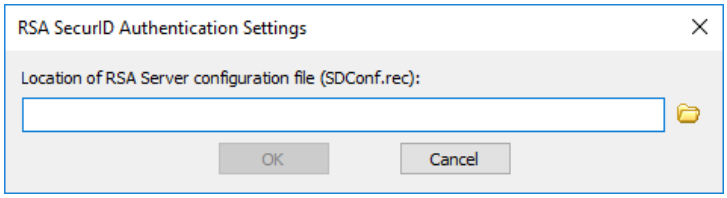
- Configuring RSA SecurID on an Existing Site

Configuring RSA SecurID Support on an Existing Site

EFT can be configured for RSA SecurID authentication via either Native SecurID protocol or RADIUS. (Requires AAMM.) To configure RADIUS on a new Site, refer to Defining Connections (Sites). For more information before configuring, refer to RADIUS for User Authentication.

To configure EFT for RSA SecurID

1. If you are using the RSA Native SecurID protocol, use the RSA Security Console to generate the **sdconf.rec**configuration file, then copy the file to a location on EFT (typically %windir%\system32).
2. Log in to the EFT administration interface and click the Site node for which you want to enable RSA SecurID.
3. Click **RSA SecurID**and then click **Configure**. The **RSA SecurID Authentication Settings**dialog box appears.
4. The **RSA SecurID Authentication Settings** dialog box is available from each Globalscape, AD, LDAP, or ODBC-authenticated Site. The dialog box allows you to specify the location of the RSA Server configuration file.



5. Click the folder icon to specify the location of the RSA Server configuration file (**sdconf.rec**). Note that SecurID files will reside in this location. **Node secret** and **sdstatus.12**files will be generated at this location. When configuring RSA in an HA environment be sure to have the sdconf.rec file store locally for each node. Each node MUST have its own copy of sdconf.rec.
6. Click **OK**.
7. Click **Apply**to save your settings.
8. Click **Yes**to restart the Site.

RSA SecurID uses a “sdconf.rec” file to configure itself as an authentication agent. Upon initial connection to the SecurID server (the first authentication attempt), a "shared secret” is established between (the Authentication Agent (EFT) and the RSA SecurID server. EFT saves this secret in the same path as the Site's “sdconf.rec” file. If you clear the node secret in RSA SecurID, you will need to clear the secret on EFT, or it will be unable to establish a new one with the server. While the service is stopped, delete the “sdstatus.12” and “securid” files that EFT created. When you restart the service, a new secret is established.

When using HA, **you need to specify a unique location (local) for the log files**. This is for troubleshooting purposes (to know on which node the issue occurred). Also, having two nodes write to the same file causes issues with file locking, which will cause data in the logs to be lost. For visibility into node status, enable cluster logging. Logging.cfg has new logging options specifically for HA. When configuring RSA in an HA environment be sure to have the **sdconf.rec**file stored locally for each node. Each node MUST have its own copy of sdconf.rec.

Related Topics

- RADIUS for User Authentication
- Enabling or Disabling RADIUS

RADIUS for User Authentication

(Included in Advanced Authentication Modes Module) Remote Authentication Dial In User Service (RADIUS) is a networking client/server protocol that runs in the application layer, using UDP as transport, and provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect to and use a network service. EFT has been extended for RADIUS support for RSA SecurID® two-factor authentication to send and receive RADIUS packets to/from a RADIUS server for user authentication. RADIUS authentication can be added to Globalscape, Active Directory, LDAP, and ODBC-authenticated Sites in the EFT administration interface. The RADIUS settings allow you to configure EFT as a Network Access Server (NAS).

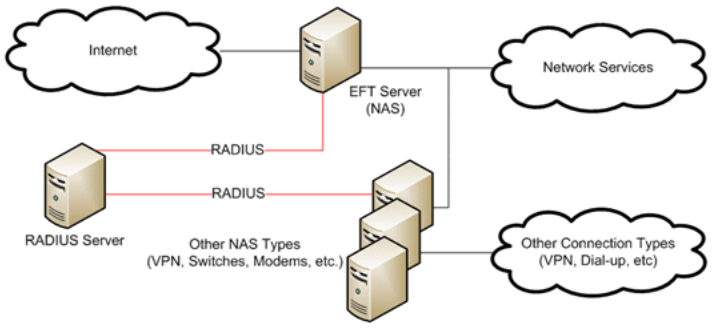
RADIUS and RSA SecurID cannot run together on the same Site. EFT does not support password reset and aging policies for RADIUS or RSA-enabled Sites.

How does RADIUS work with EFT?

The user or device sends a request to EFT to gain access to a particular network resource, then EFT sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol. The request may contain username, password, security certificate, network address, and IP/Port used to connect to EFT. RADIUS servers vary, but most can look up client information in text files, AD/LDAP servers, or databases. The RADIUS server can respond with an Access Reject, Access Challenge, or Access Accept. If the RADIUS server responds with an Access Challenge, additional information is requested from the user or device, such as a secondary password.

In the Web Transfer Client, after the user authenticates with their EFT, AD, or LDAP credentials, they are asked for their RADIUS/RSA SecurID authentication. The account configured in EFT must match the user account on the RSA server. Whatever the user provides to log in to EFT is sent to the RSA server. For LDAP authentication, sAMAccountName should be configured.

The diagram below provides a general overview of EFT configured in a network with RADIUS.

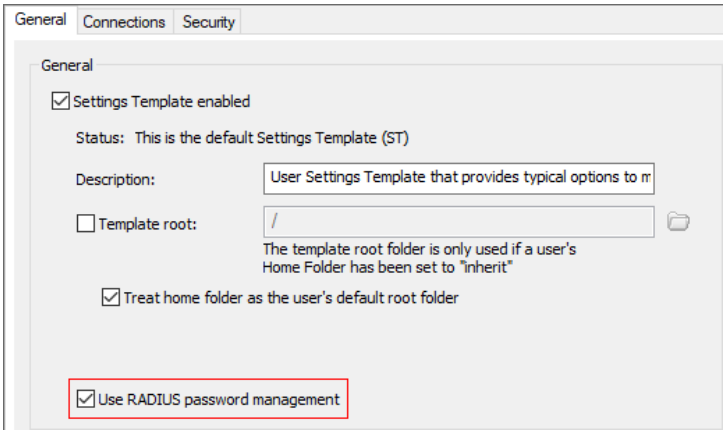


How do I configure RADIUS in EFT?

You configure RADIUS in the EFT administration interface. The EFT Authentication Manager, Settings Templates, User Settings, New Site wizard, and New User Wizard each allow RADIUS configuration.

In Globalscape, LDAP, AD, and ODBC-authenticated Sites, the **RADIUS Authenticated Settings** dialog box, accessed from the **New Site** wizard and/or the Site's **General**tab, allows you to enable RADIUS or RSA SecurID authentication and to configure the RADIUS/RSA server's IP address, port, NAS Identifier, shared secret, connection retries, and timeout.

On the Settings Template and user account **General** tabs, and in the **New User** wizard, a **User RADIUS password management**check box is provided for those instances where you might want the Site to have RADIUS enabled, but want to disable it for a Settings Template or specific user.



Supported Protocols

EFT supports RADIUS and RSA SecurID authentication for FTP, FTPS, SFTP, HTTP and HTTPS.

- AS2 does not support interactive authentication.
- EFT does not perform inline checking for PCI DSS compliance for various password controls. In PCI DSS reports, a **Status**value labeled "Compensating Control" and the following Compensating Control text appears: "Compensating Control: User authentication and password controls for %WHO% are being managed by a remote system, such as RSA SecurID®. (The %WHO% variable contains the name of the Site, Settings Template, or user account.)

Related Topics

- Using SFTP/SSH with Radius/RSA Servers
- For details of configuring RADIUS on a new Site, refer to Defining Connections (Sites).
- For details of COM API methods for RADIUS, refer to "Creating a User" (CreateUser and CreateUserEx) in the COM API Reference.

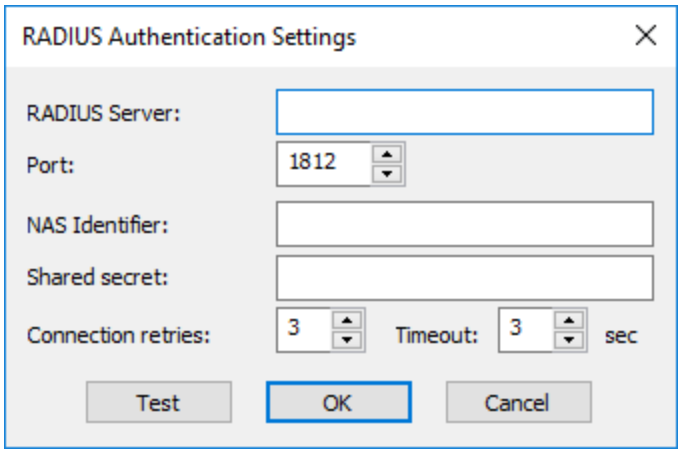
Configuring RADIUS Support on an Existing Site

EFT can be configured for RADIUS authentication. (Requires AAMM.) To configure RADIUS on a new Site, refer to Defining Connections (Sites).

For more information before configuring, refer to RADIUS for User Authentication.

To configure EFT for RADIUS

1. Log in to the EFT administration interface and click the Site node for which you want to enable RADIUS.
2. Click **RADIUS**and then click **Configure**. The **RADIUS Authentication Settings** dialog box appears.



The dialog box allows you to enable and configure the connection to the RADIUS server

   a. **RADIUS Server**—Specifies the name of the RADIUS Server (host name or IP address).
   b. **Port**—Specifies the port the RADIUS Server is bound to. The default port is 1812.
   c. **NAS Identifier**—Specifies EFT's NAS identifier for the RADIUS Server.
   d. **Shared secret**—Specifies the shared secret used to encrypt and sign packets between EFT and the RADIUS Server.
   e. **Connection Retries**—Specifies the number of times a RADIUS packet will be submitted to the server before giving up. The packet is resubmitted if there is no response from the server. (RADIUS runs over UDP, so packets may be dropped or ignored by the server). The default is 3 retries.
   f. **Timeout**—Specifies how long to wait for a server response, in seconds. The default is 3 seconds.

3. Click **OK**.

4. Click **Apply**to save your settings.
5. Click **Yes**to restart the Site.

Related Topics

- RADIUS for User Authentication
- Enabling or Disabling RADIUS

Enabling or Disabling RSA Authentication via RADIUS

(Included in Advanced Authentication Modes Module) If RADIUS is enabled on a Site and a Settings Template, you can enable or disable the use of RADIUS for individual user accounts. (The username must correspond to a username in the RSA Authentication Manager server's database.) For example, you may have some users who will use RADIUS to authenticate on the Site, but other user who do not use RADIUS. (You cannot enable RADIUS authentication for user account on a Settings Template or a Site that does not have RADIUS authentication enabled or defined.)

To enable or disable RADIUS for a user account

1. On the **Server** tab, in the tree of a Site that has RADIUS enabled, expand the Settings Template of users for whom you want to enable or disable RADIUS.
2. In the right pane, on the **General** tab, clear the **Use RADIUS authentication** check box to disable RADIUS; select the check box to enable RADIUS.
    - You can also enable or disable RADIUS in the **New User** wizard when you create the user account.
3. Click **Apply** to save the setting.

On user accounts that have RADIUS enabled, it is possible for users to lock themselves out of the RADIUS server (for example, due to multiple invalid logins). The user in this case will not be able to log in to EFT, but will not appear to be locked out of EFT in the administration interface. EFT will log only that a login was denied at the protocol level (on INFO in HTTP). You must unlock the account on the RADIUS server for the user to be able to log in to EFT. (For information about unlocking accounts on the RADIUS server, refer to that server's user guide.)

SAML (Web SSO) Authentication

The HTTP and HTTPS protocols in EFT provide the Security Assertion Markup Language (SAML) 2.0 Web Single Sign On (SSO) profile with HTTP POST binding and corresponding user interface controls for enabling and configuring SAML for achieving SSO for Web-based authentication. (Requires Advanced Authentication Modes Module (AAMM).)

The topics below provide information regarding SAML Authentication.

- Introduction to SAML (Web SSO) Authentication
- Configuring a Site for SAML
- SAML Scope
- Tools for Debugging SAML Communications
- Web SSO Error Handling
- SAML-Related Knowledgebase Articles

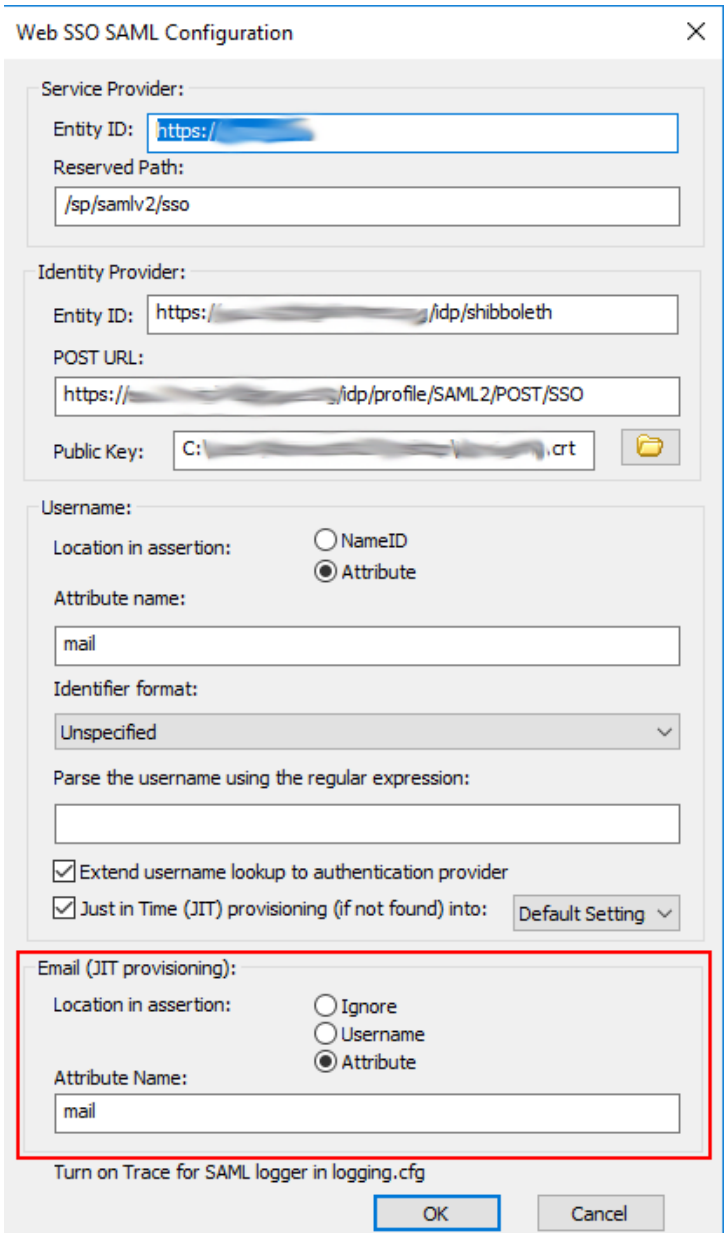
Introduction to SAML (Web SSO) Authentication

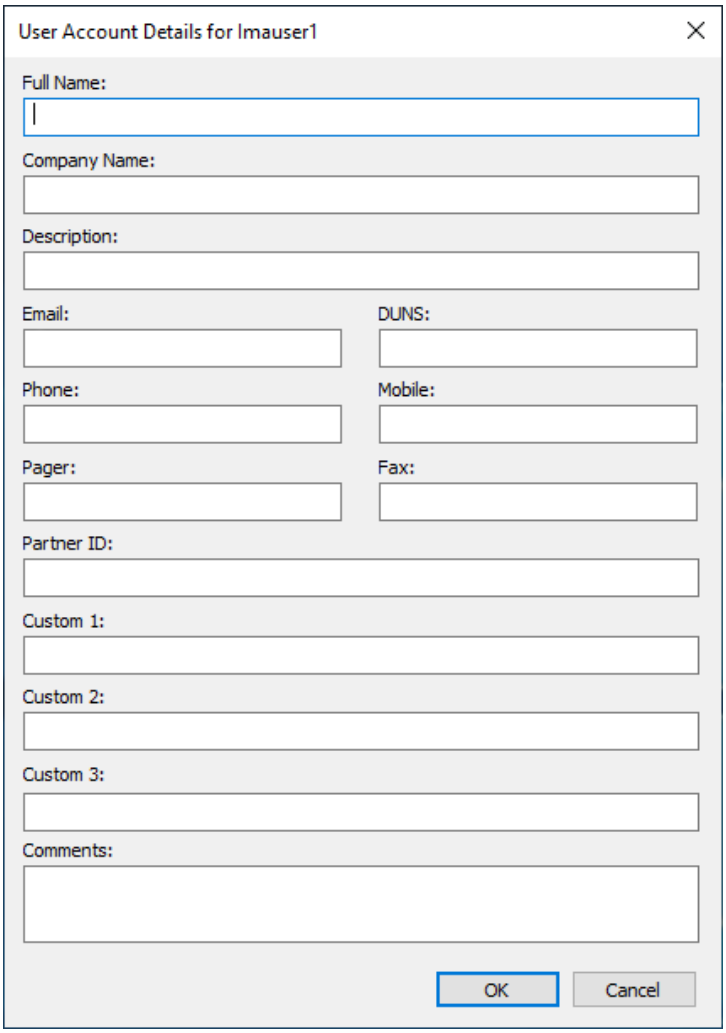
(Requires AAMM) The SAML SSO feature in EFT will look up accounts to match the user-id configuration, and if found, it will associate the IdP-authenticated users with said pre-provisioned accounts. EFT can also optionally perform what's called Just In Time (JIT) provisioning, where it can create an account in a pre-designated Settings Template, for authenticated users, if they do not already exist in EFT. When a positive mapping of identify assertions to existing user accounts cannot be made, Web SSO authentication will fail or revert to normal authentication and request login credentials. (See Web SSO Error Handling).

In the **Web SSO SAML Configuration** dialog box, you can specify to use the Email Attribute Name in JIT or LDAP after an IDP- or SP-initiated login to create an account in EFT.

When Web SSO is enabled for a Site, and if the **Persist username and password credentials for use in Event Rule context variables** check box is selected, EFT displays the WARNING prompt shown below. Some users will be able to login normally (if desired), thus the "persist credentials" feature *could* work in those cases, which is why it isn't automatically disabled when SSO is enabled.

> **WARNING:** The "persist credentials" feature will not work for accounts that login via Web Single Sign-on (SSO), because there will be no credentials to persist. Instead, you would have to manually specify those credentials for each rule. If you leave the persist credentials feature enabled (or if was already enabled), then EFT will use an empty (NULL) password.


Web SSO SAML Configuration
Service Provider:
Entity ID:
https:/
Reserved Path:
/sp/samlv2/sso
Identity Provider:
Entity ID:
https:/
/idp/shibboleth
POST URL:
https://
/idp/profile/SAML2/POST/SSO
Public Key:
C:
.crt
Username:
Location in assertion:
NameID
Attribute
Attribute name:
mail
Identifier format:
Unspecified
Parse the username using the regular expression:
Extend username lookup to authentication provider
Just in Time (JIT) provisioning (if not found) into:
Default Setting
Email (JIT provisioning):
Location in assertion:
Ignore
Username
Attribute
Attribute Name:
mail
Turn on Trace for SAML logger in logging.cfg
OK
Cancel

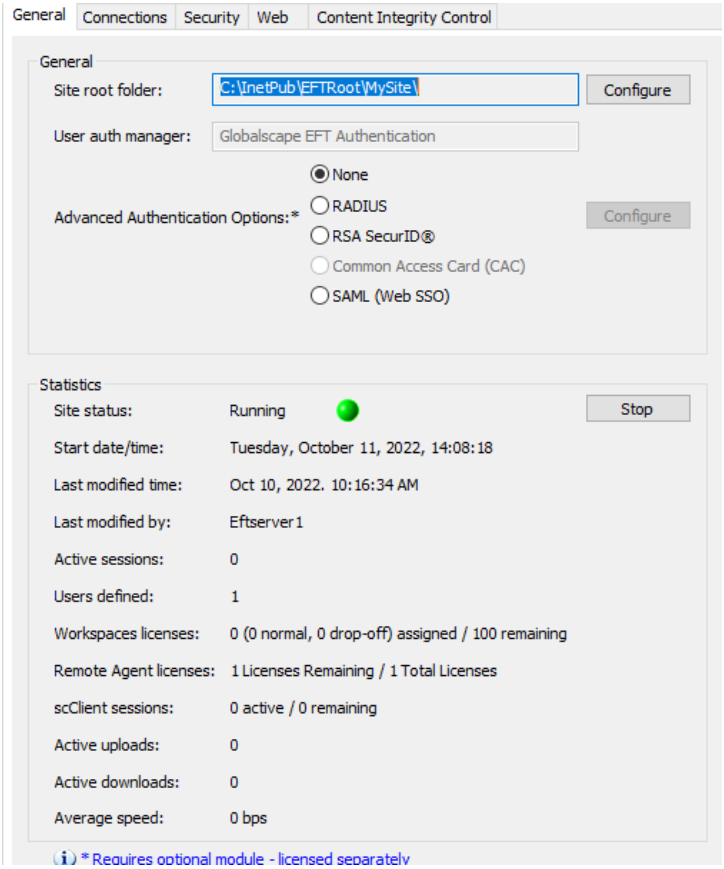


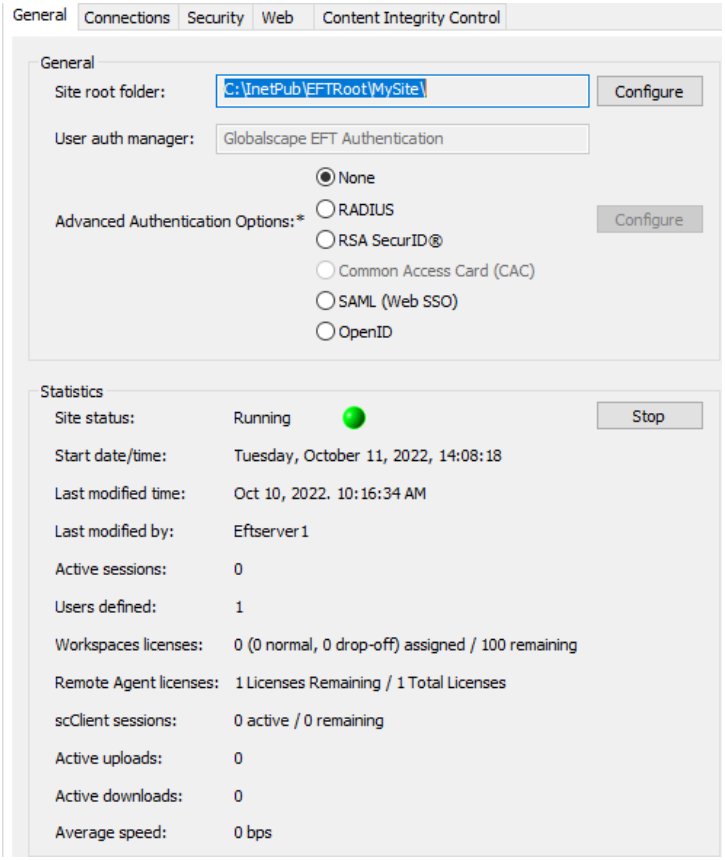
- Web SSO support in EFT is limited to LDAP, ODBC, and Globalscape-authenticated Sites; Web SSO is **disabled and unavailable for AD**-authenticated Sites.
- SAML 2.0 Service Provider-initiated Web Single Sign-on with POST bindings is currently the only profile supported on EFT. EFT uses the OpenSAML library SAML 2.0. EFT does not support SAML 1.0 or 1.1.
- When EFT is installed in an HA environment, SAML needs to have the IDP's public key saved in the HA shared drive.
- EFT **Login Security** options do not apply to SSO failed logins. Login security controls, such as password complexity and failed logins, are within the responsibility of the Identity Provider (IdP) and are not controlled by EFT. (Refer to Banning an IP Address that Uses an Invalid Account and Disabling or Locking out an Account after Invalid Password Use for details of those options.)

Configuring a Site for SAML (Web SSO) Authentication

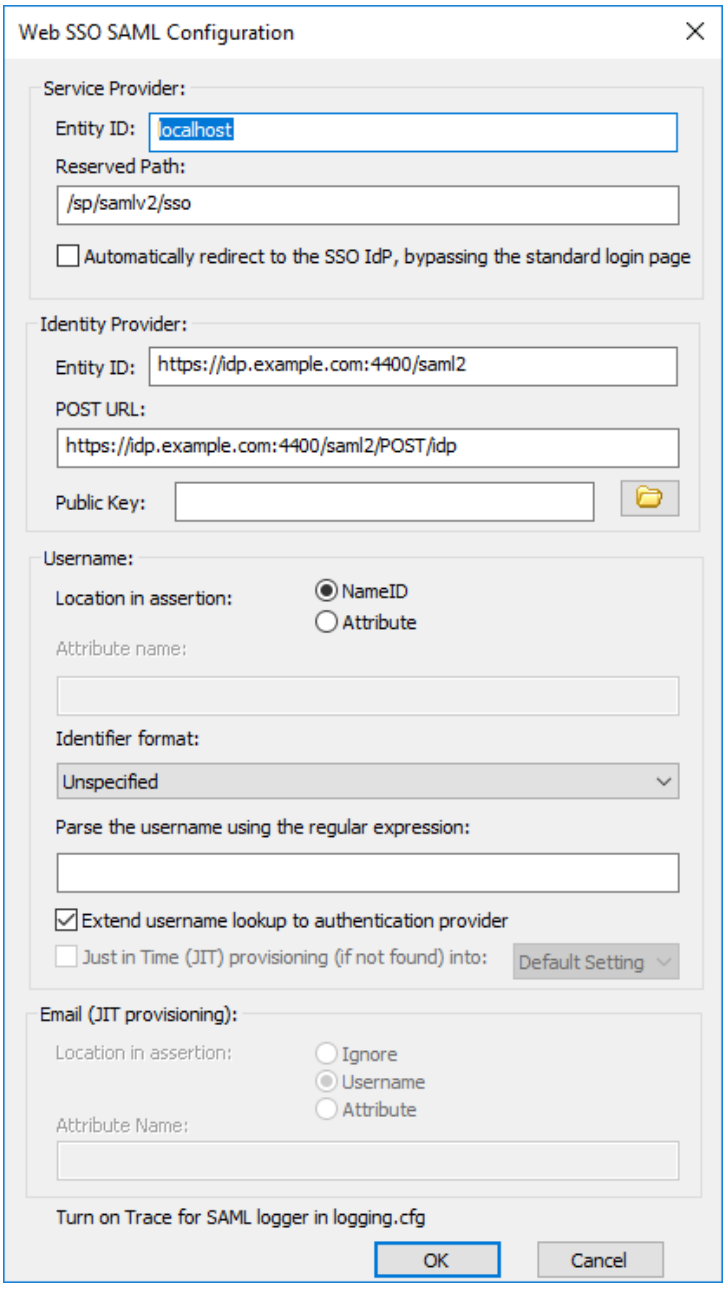
To enable SAML (Web SSO) authentication (Requires AAMM)

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **General**tab.





4. Click **SAML (WebSSO)**, click **Configure**, then provide the details needed to configure SAML.



a. **Service Provider:**

- **Entity ID**- The default is the host name value specified for the EFT Site being configured, e.g., MySite. Any string value can be provided, up 255 characters, including UTF-8 encoded characters.

- **Reserved Path** - The base address followed by the SSO path, e.g., [hostaddress]/sp/samlv2/sso. (Leaving the box blank or as root path ("/") is not allowed. You will receive an error message and configuration will not be saved. (Upon upgrading to 8.0.4 or later, the Reserved path will be changed to **https:///sp/samlv2/sso** and the **Automatically redirect to the SSO IDP** check box will be selected.)
- **Redirect to the SSO service, bypassing the standard login page**- When selected, EFT will redirect to the SAML IdP from the WTC login page.

  If the **Automatically redirect to the SSO IDP**check box is selected, it may result in redirect failures under certain conditions and with certain browsers, which can only be overcome by setting the "HTTPCookieSameSitePolicy" Advanced Property to "Lax".

b. **Identity Provider**:
   - **Entity ID** - The Identity Provider's host name
   - **POST URL** - The Identity Provider's POST URL or endpoint that EFT should bind to.
   - **Public Key** - Certificate path to be used for verifying the server's identity

c. **Username**:

   The LDAP User attribute must match the **Identifier**attribute selected in the **Web SSO SAML Configuration** dialog box.

   - **Location in assertion** - Specify whether the username is stored as **NameID** or **Attribute**.
   - **Attribute name** - If Attribute is specified for location, provide the Attribute name.
   - **Identifier format** - Select the list box and click the format identifier from the list:
     - Unspecified
     - Email Address
     - X.509 Subject Name
     - Windows Domain Qualified Name
     - Kerberos Principal Name
     - Entity Identifier

- URI Reference
- Basic

d. **Parse the username using the regular expression** - Use wildcards to parse the username. For example, to take everything to the left of the @ sign in an email address (typically the username), type or paste the following regular expression into this box: ^(.*)@.*

> **NOTE:** EFT uses the regular expression engine in .NET.

e. **Extend username lookup to authentication provider** - Specifies that EFT should perform lookup of recipients in both EFT and LDAP. (Query LDAP in addition to users in EFT.) The check box is selected by default for new installations.

f. To enable **Just in Time (JIT) provisioning** of users, select the check box, then specify whether users are to be created in the **Default**Settings Template or the **Guest Users** Settings Template. If enabled, EFT will auto-provision (create) authenticated users in the Globalscape authentication database if they are not already present on that Site. Workspaces must be enabled for the **Guest Users** template to show under JIT provisioning.

g. Under **Email (JIT provisioning)** specify the location of the email in the assertion:

- Ignore the email from the assertion provided by the IdP
- Reuse the username
- Look up a specific attribute.

EFT will not update the email field if it is already populated or is null, other than upon initial provisioning of the user account.

5. Click **OK**. Turn on "Trace" for `SAMLSSO`logger in logging.cfg.

SAML Scope

(Requires AAMM) EFT follows the reference implementation for SAML 2 according to http://docs.oasis-open.org/security/saml/v2.0/with the following constraints in place.

1. **SAML 2.0 only:**No support for SAML 1.1 or earlier.
2. **Web Profile only:**No support for thick client access using SSO.
3. **POST binding only:**EFT is limited to HTTP's POST method for binding to the IdP endpoint.
4. **Auth assertions only:**EFT as a Service Provider (SP) is limited to requesting that the identity provider (IdP) authenticate a user principal (subject) and processing of the IdP authentication assertion.
5. **Limited identity management providers:** EFT's Web SSO support for identifying authorized users (for subsequent authorization and home directory assignment) is limited to LDAP, ODBC, and Globalscape (EFT's built-in) authentication providers, and thus will be disabled and unavailable for native AD authentication (as native AD will authenticate the user, thus obviating the need for SAML); however, LDAP sync against an AD will be allowed for confirming the user's identity).
6. **No JIT:** EFT's Web SSO feature does not support just in time (JIT) provisioning of user accounts, instead relying on accounts already being provisioned in EFT (via one of the above supported identity providers), failing authentication outright or reverting back to normal authentication methods (request login credentials) when a positive mapping of identify assertions to existing user accounts cannot be made, subject to administrator configuration option to this effect.
7. **No credentials persistence:**When Web SSO is enabled for an EFT Site, and if under **Site > Security**tab the **Persist username and password credentials for use in Event Rule context variables** is toggled on (checked) by the administrator, EFT will not be able to persist credentials to its event rules (as there are none).
8. **No logout redirect:**EFT does not provide support for a logout redirect URL or support the Single Logout Protocol (3.7 in SAML Core 2.0 spec). Instead when the user logs out (from the WTC) EFT will expire their EFT web session and place them on the main logon page, e.g. the WTC logon page. Users can click on the SSO login button or navigate to the SSO reserved path to re-POST to the IdP all over again.

SSO Process

(Requires AAMM)

1. If SAML is **enabled**and a **connection is made** to the SAML reserved path or the SSO button is clicked on the WTC login page, EFT will perform a POST binding to the predefined IdP. See Configuring a Site for SAMLfor configuration of these options.
2. EFT subsequently communicates its **Entity ID** and will verify the issuer's Entity ID upon receiving an assertion from the IdP.
3. The IdP, if configured with EFT's information (including certificate info) will validate EFT's **request message signature** and process the request POSTed by EFT.
4. The IdP will next **authenticate**the user directly using whatever mechanism it was configured to use for authentication (cert, user+pass, 2FA, other), or forward the request upstream to another IdP, or rely on a cached session. Whichever the case, the IdP should authenticate a user it trusts and return a response containing an assertion to EFT.
5. EFT will validate the IdP's **response message signature**, if signed, using the IdP's pre-configured public key. If the response signature is valid it will read the assertion. If not valid, EFT will deny the claim and return an error. IdP response message signatures are optional.
6. EFT will also validate the **assertion signature** using the IdP's pre-configured public key. If the assertion signature is present and valid, EFT will perform a username lookup, otherwise it will return an error. Assertion message signatures are required.
7. EFT will also decrypt the assertion if encrypted. If decryption using the EFT site's private key succeeds, EFT will proceed to perform username lookup, or if decryption fails, EFT will deny the claim and return an error. Encryption of assertions within the IdP response is optional.
8. EFT will then check and validate the following claims made in the assertion:
    a. **NotBefore**- Claim isn't valid prior to the time specified (see clock skew).
    b. **NotOnOrAfter**- Claim is not valid on/after time specified (see clock skew).
    c. **OneTimeUse**- Don't cache and reuse claim.
    d. **AuthzDecisionStatement**- if Deny or Indeterminate as Decision Type then reject claim
    e. **StatusCode**- Reject if anything other than status:Success

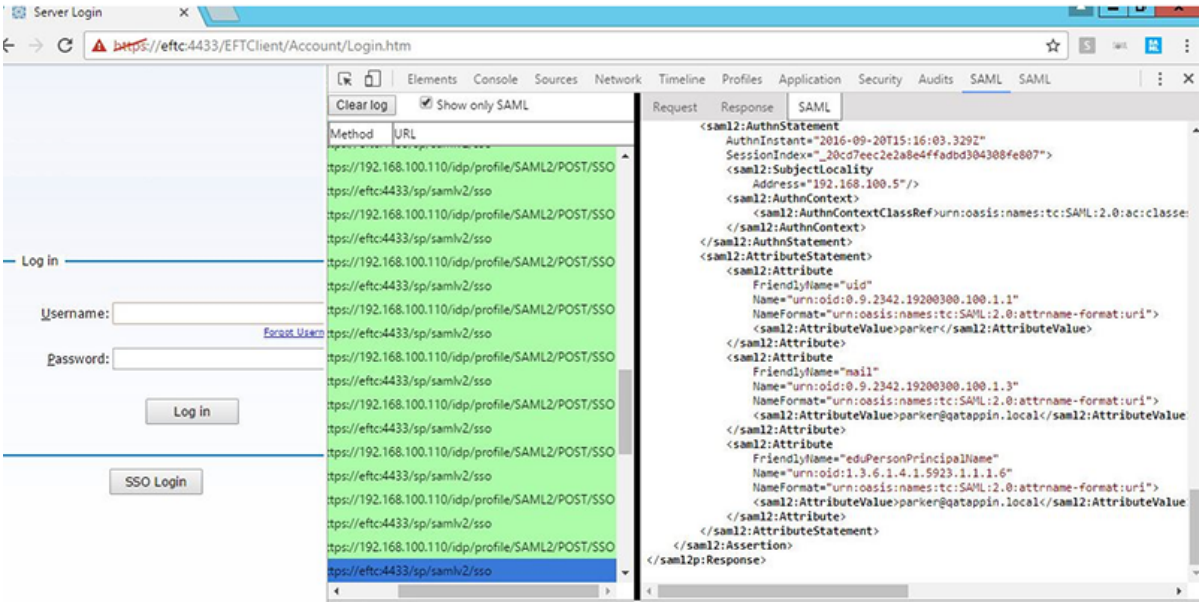
9. If EFT cannot evaluate, parse, or understand a sub-element or attribute of the Conditions element then the entire assertion is considered invalid. This is to adhere to SAML 2 protocol.

10. EFT will next look up the **user identity** in the claim and attempt to match that username to an existing account in EFT (obtained via directory services called to LDAP, ODBC, or Globalscape authentication provider). If EFT finds an exact match then it knows that the user exists in EFT, where to place that user (their home folder), and what permissions to give that user.
11. If rejected, the user will see an **error**and be redirected to the logon page (where they can enter their credentials), or if the SAML reserved path was set as the root path (e.g. “/”), then they will be redirected to the logout page (otherwise it would result in an endless loop of authentication attempts). "Failed to find, unambiguously match assertion subject to existing and enabled account."
12. EFT includes a predefined IdPSP time offset skew of 180,000 milliseconds (3 minutes) for claim validity in either direction, along with an advanced property where the administrator can specify smaller or larger values, capped internally at unsigned INT (0 to 4,294,967,295) ms. This allows for case where IdP and SP's clocks are not in sync and the assertion has a time window that either causes the user not to be able login until some point in the future, or causes their claim to expire prior to being able to login with regard to the service provider.

Tools for Debugging SAML Communications

(Requires AAMM) When setting up and testing SAML communications between the SP (EFT) and your IdP, you may need to review assertions, especially if authentication is failing for some reason. There are two ways you can do this:

1. In EFT's logging.cfgfile, uncomment Trace logging for `log4cplus.logger.SAMLSSO`.
2. Perform any test communications (attempt to establish a session), then open EFT.log and review the trace log output.
3. In Google Chrome, there is a developer tool add-in called SAML Message Decoder that will permit you to easily sniff SAML requests and responses made to the IdP, that occur when the user clicks the **SSO Login** button on WTC's home page, or if navigating to the SSO reserved path.



Validate Username Regex

EFT must be configured so that it can extract the username from the assertion, so it can attempt a match of the pre-defined user accounts in EFT you pulled down from LDAP or other authentication manager. If EFT cannot find a match, it will be because the user does not exist in its username store, or you've misconfigured the username regex matching and EFT is failing or improperly parsing the username from within the assertion.

> **NOTE:** EFT uses the regular expression engine in .NET.

You can attempt to do the following to ensure proper regex mapping:

1. Configure your IdP (such as Shibboleth) to return the user attribute mail in the format of username@domain.com
2. Configure your IdP and EFT to match on the username attribute value of “mail”.
3. Under the “Parse the username using the regular expression” field to grab everything to the left of the @ field: ^(.*)@.*
4. Ensure there is an EFT user that matches on the username, without the email address, e.g. “username”.
5. Attempt to login with that user. If it fails, refer to the debugging section above.
6. There are several online tools that can aid you in creating and testing out your regex expressions: https://regex101.com/

Generate SP Metadata File

Identity Providers (IdPs) need a way to know which Service Providers (SPs) they can trust. IdPs are informed of trusted SPs either via manual configuration or by importing the SP's information using a metadata file, which is an XML formatted file that contains all of the relevant SP information (public key, Entity ID, etc.). At this time, EFT does not produce the metadata automatically, nor can it import the IdP's metadata (thus requiring that you manually configure EFT's SAML settings in EFT); however there are tools, including an online tool and one provided by ADFS that you can use to generate a metadata file from EFT's SAML configuration that you can then import into your IdP of choice.

Prerequisites:

1. Ensure that SAML / Web SSO is enabledin EFT.
2. Ensure that you have enabled HTTPS in EFT
3. Ensure that you have already created an SSL certificate in EFT

Generate Metadata Using SAML Tool's Metadata Generator

1. Run the tool from https://www.samltool.com/sp_metadata.phpand use the settings described below.
2. **EntityId—Enter**the value in EFT's Entity ID field under Web SSO config.
3. **Attribute Consume Service Endpoint (HTTP-POST)**—Enter the combined values from under Entity ID and Reserved Path, e.g. https://[domain]/sp/samlv2/sso
4. **Single Logout Service Endpoint (HTTP-REDIRECT)**—Leave blank.
5. **SP X.509 cert block**—Browse to EFT's configuration path (the default is C:\ProgramData\Globalscape\EFT Server\ ), open the SSL certificate public key that you created for HTTPS, and copy the key blob into that field. This should look like a long string of numbers and characters.
6. **NameID Format**—Leave as is or change to desired value.
7. **AuthnRequestSigned**—Change to True if desired, as EFT always signs its request.
8. **WantAssertionsSigned**—Set to true, for greater security. EFT supports both.
9. All the other fields are optional.
10. Click **BUILD SP METADATA**.
11. Copy the metadata into a text file and name it appropriately, e.g. eft_saml_ metadata.xml.
12. Import your metadata into your IdP.

Related Topics

- SAML-Related Knowledgebase Articles (Including tips for configuring IDPs)

Web SSO Error Handling

When Web SSO is enabled for a Site, and if the **Persist username and password credentials for use in Event Rule context variables** check box is selected, EFT displays a WARNING prompt:

> **WARNING:** The "persist credentials" feature will not work for accounts that login via Web Single Sign-on (SSO), because there will be no credentials to persist. Instead, you would have to manually specify those credentials for each rule. If the persist credentials feature is enabled, then EFT will use an empty (NULL) password. (Some users will be able to login normally (if desired), thus the "persist credentials" feature *could* work in those cases, which is why it isn't automatically disabled when SSO is enabled.)

Refer to Using Login Credentials in Event Rules for more information about that setting.

Related Knowledgebase Articles

- 11321, EFT SAML SSO with Salesforce as IDP
- 11322, Installing and configuring Shibboleth as the backend IDP server for use with EFT SSO
- 11323, Configure SafeNet to accept EFT for SAML IDP access
- 11324, Creating and configuring an ADFS IDP server for use with EFT SAML
- 11330, Adjust clock skew between EFT and IDP server
- 11331, Specify the SAML signature algorithm
- 11332, Specify the SAML digest algorithm
- 11433, Ignore or Enforce the SAML Assertion Signature or SAML Message Signature

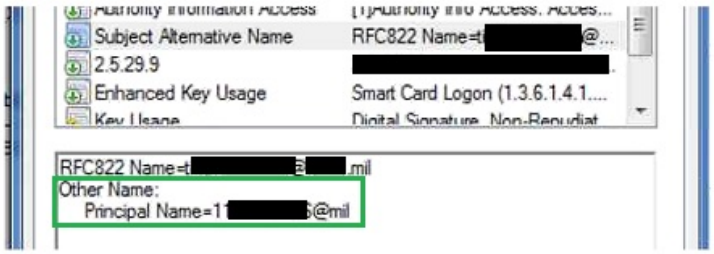
Common Access Card Authentication

Common Access Card (CAC) Authentication is available for LDAP Sites with SSL (HTTPS or FTPS) enabled. (Requires Advanced Authentication Modes module.)

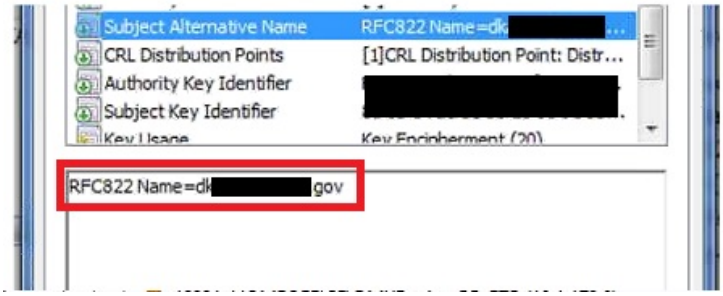
CAC and Certificates

When CAC is enabled on an LDAP Site, clients are required to provide a certificate when connecting. Once the user's certificate is validated, EFT uses the Principal Name (UPN) or RFC822 Name taken from the Subject Alternative Name (SAN) field of the Signature Certificate to search for the user in LDAP and allow or deny access based on the information found. The certificate provisioned via the web browser must have an Electronic Data Interchange Personal Identifier (EDI/PI). If the EDI/PI is not found or otherwise cannot be validated, the connection is denied. If the EDI/PI is found, EFT maps the corresponding fields in LDAP using the appropriate LDAP query string. If the user is found in LDAP, if a certificate is assigned to that user, and if the certificate exactly matches the one provided by the client, the user is allowed access.

Valid CAC cert format



Not valid CAC cert format



The certificate lookup process looks like this:

1. EFT looks for UPN or RFC822 Name entry in SAN field of certificate (that is, the OID)
2. EFT performs an LDAP lookup using the LDAP Auth Manager specifications, searching against the user login attribute for the value found in the entry of SAN.

3. This lookup returns 0 or more "userCertificate" properties of the matched object, if found.
4. For each returned userCertificate, EFT does a cryptographically strong comparison of the LDAP-provided certificate and the one supplied by the CAC.

CAC and WTC

- The account management page is not available when CAC is enabled. There is no concept of logging out or changing passwords when using CAC.
- CAC is only available on an LDAP-authenticatedSite.
- CAC is incompatible with RADIUS, RSA, PCI DSS, ODBC, NT authentication, AD authentication, and Globalscape authentication. PCI DSS Compliance reports do not report on CAC-enabled Sites.
- Refer also to Knowledgebase article #11329, Enabling Workspaces for external users on CAC-enabled Site
- EFT v8.x does not support UPLOADS from CAC-authenticated users when using Chrome or Edge browsers. Firefox (and possibly other browsers) will work.

When CAC is enabled on a Site:

- Any attempt to access any of the account management pages causes a "page not found" error.
- When HTTP and HTTPS are both enabled, the **Redirect HTTP to HTTPS** check box is selected and disabled, forcing redirection of HTTP traffic to HTTPS.
- When FTPS is enabled, the username and password provided are ignored; the authentication is provided by the certificate.
- The method `EnableCAC()` can be used to enable CAC via the COM API.
- The following major events are logged:
  - Could not find proper SAN field in certificate
  - The value received from the SAN field
  - If user had no certificates in LDAP
  - If certificates were present but no certificate matched
  - More than one user was retrieved when LDAP was queried (authentication is only attempted against the first one)

Related Topics

- Configuring CAC on an Existing LDAP Site
- Defining Connections (Sites) for details of creating an LDAP-authenticated Site that uses CAC.

- Guidelines for enabling smart card logon with third-party certification authorities (Microsoft Support article)

Configuring CAC on an LDAP Site

EFT can be configured for Common Access Card (CAC) authentication. (Requires AAMM) To configure CAC on a new Site, refer to Defining Connections (Sites). For more information before configuring, refer to Common Access Card (CAC) Authentication. EFT v8.x does not support UPLOADS from CAC-authenticated users when using Chrome or Edge browsers. Firefox (and possibly other browsers) will work.

To configure EFT to use CAC Authentication

1. Log in to the EFT administration interface and click the LDAP Site node for which you want to enable CAC.
2. On the **General**tab, in the **Advanced Authentication Options** area, click **Common Access Card (CAC)**.
3. Click **Apply**to save your settings.
4. Click **Yes**to restart the Site.

Related Topics

- Common Access Card (CAC) Authentication
- Defining Connections (Sites)

Advanced Workflow Module

With EFT Event Rules, you can configure EFT to perform an Action automatically when a specific Event occurs. You can use Advanced Workflows to design scripts, batch files, macros, or any other code-intensive process using an easy drag-and-drop interface, and than add the Workflow to one or more Event Rules. Advanced Workflow Task names can appear in reports and logs.

The topics below describe using the Advanced Workflow actions specifically in EFT Event Rules.

> **NOTE:** For details of the Advanced Workflow actions, please refer to the help documentation in the Task Builder in the EFT administration interface. The help documentation for Advanced Workflow Actions can also be found in the installation folder for AutoMate: **C:\Program Files\Globalscape\AutoMate\Help\Default.htm**.

- What's New in the AWM?
- Installing or Upgrading the Advanced Workflow Module
- Upgrading the Advanced Workflow Module
- Automate Service Account
- Introduction to Advanced Workflows
- Advanced Workflow Concepts
- The Task Builder Interface
- Advanced Workflows Features and Benefits
- The Workflow Task Builder Overview
- Creating Workflows for use in an Event Rule
- Creating Workflow Folders
- Sample Workflows
- Advanced Workflow Variables
- Workflow Conditions
- Backing Up Workflows
- Importing and Exporting Advanced Workflows
- Encrypt Files in a Workflow Using EFT OpenPGP Key
- Technical Reference
- Knowledgebase Articles about the Advanced Workflows

What's New in the AWM?

The Advanced Workflow Module uses components from Fortra's Automate Desktop, which is bundled in the EFT installer. This topic discusses changes from Automate 10 (the previous version bundled in the EFT installer) and Automate 2024.

IMPORTANT: Before installing Automate 24.x or Automate Desktop 24.x, confirm your version of Windows is compatible with .NET Framework 4.8.

New Features

- 64-bit installer (As of version 11.7.1, Automate is only available as a 64-bit installer.)
- Dataset
  - Adds the ability to create and manipulate datasets, as well as manage the rows and columns within them.
- JSON Object
  - JSON Decode - convert a JSON-encoded string into Automate variable engine objects.
  - JSON Encode - convert an Automate variable engine object into a JSON-encoded string.

Enhancements

- Added support for Windows Server 2022
- Azure Action Enhancements
  - The Azure Action has been updated to support TLS 1.2.
- SharePoint Action Enhancements
  - SharePoint activities can now pull over information from multi-choice Lookup, User, and Group columns to populate datasets.
  - Added Azure AD Delegated and Interactive authentication types to support multifactor authentication (MFA) and single sign-on (SSO) with SharePoint Online-based connections.
  - Added SharePoint App Only and Azure AD App Only authentication types to support modern authentication with SharePoint Online.
  - Removed support for SharePoint 2007 and 2010 from the SharePoint action and SharePoint Browser.

  - Added the "Preserve internal column names" parameter to the SharePoint (Get files, Get Folders, and Get list item(s)) activities which provides the option to prevent SharePoint columns from being renamed in datasets.
  - SharePoint activities now correctly fail if user credentials are not valid.
  - The SharePoint (Get folders) activity no longer displays the "Error VirusStatus column already exists" error message during runtime for SharePoint 2019 and Online-based connections.
  - The SharePoint (Upload file(s)) activity now provides the option to set metatags while uploading files and retrieve uploaded file IDs.
  - The SharePoint Condition no longer displays a "not supported" error when set to "Evaluate condition immediately."
  - The SharePoint Trigger now properly fires tasks and workflows.

    > **NOTE:** The SharePoint trigger has been updated to use Transmission Control Protocol (TCP). The default TCP port is 9705. If you need to change this port number, please contact Fortra Support.

- Variable Action Enhancements
  - Added the ability to add a variable to the Watchlist by right-clicking on it from the Variables pane in the Task Builder.
  - Numeric-type variables are now handled and stored in decimals to provide higher precision.
  - The Variable (Create) and Variable (Set) activities now dynamically resize the "Initial value" and "New value" fields, based on input data.
  - The Variable (Create) activity now provides the option to secure a variable which will encrypt the value of a variable while editing a task.
  - Secured variables value will still be viewable in plaintext during runtime execution.
  - Constant Values can now be assigned while creating a Task Variable.
  - The Variable Engine has been optimized to improve overall system performance.

    > **IMPORTANT:** IMPORTANT: The optimizations to the Variable Engine now require all expression functions to contain () (for example, %Now()%).

- Welcome tab
  - Added new Welcome tab to the Task Administrator in Automate Desktop and the Server Management Console in Automate Plus/Ultimate to provide quick access to important Automate community aspects — all in one place.

    - In the event the Task Administrator in Automate Desktop or the Server Management Console in Automate Plus/Ultimate become disconnected, the Welcome page will display a Connect button that allows the connection to be re-established.
- User Interface Enhancements
    - Rebranded the Automate and Automate Desktop user interfaces and company logos from HelpSystems to Fortra.
    - The user interface for Automate has been updated to provide an improved user experience.
    - Automate Desktop now displays the Automate Desktop product name in the user interface.
    - Task Builder now allows the option to automatically save tasks with an associated file every two minutes.
    - Added new UI Automation accessibility engine to support greater discoverability and ease of use when interacting with controls in desktop applications, such as Microsoft Excel.
    - Data value highlighting
    - Dockable panels
    - Variable inspector
    - Simplified event and function editing
- FTP Action Enhancements
    - The FTP (Logon) activity now supports an SSL/TLS (implicit) connection with TLS 1.0 disabled and TLS 1.1 and 1.2 enabled.
    - FTPS connections now work with TLS 1.2.
    - FTP - Logon activity now supports ECDH and ECDSA algorithms/ciphers.
    - FTP - Logon activity now supports AES (CTR,CBC) algorithms/ciphers.
    - The FTP (Upload file(s)) activity now provides the option to use multi-threaded uploads.
    - Added the ability to adjust SFTP pipeline length, block transfers, and upload/download block size.
    - Added the ability to manually adjust the "Upload buffer size (bytes)" setting for SFTP in the FTP (Logon, Download file(s), and Upload file(s)) activities.
    - Added the ability to suppress additional operations for SFTP transfers.
    - The FTP action now supports TLS 1.3 and the following TLS 1.3 ciphers:

        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384
        - TLS_CHACHA20_POLY1305_SHA256
    - The FTP action now supports the following SFTP ciphers:
        - EA_3DES was renamed to EA_3DES-CBC
        - EA_AES128 was renamed to EA_AES128_CBC
        - EA_AES192 was renamed to EA_AES192_CBC
        - EA_AES256 was renamed to EA_AES256_CBC
- OCR Action Enhancements
    - Added support for the Turkish language for all OCR activities.
    - Added support for the Tesseract engine to improve accuracy and provide more reliable results.
    - Added JPEG image format support to all OCR activities.
    - Added support for the Hebrew language to all OCR activities.
    - Added support for the Japanese language to all OCR activities.
- File System Action Enhancements
    - The File System (Move) activity's Source and Destination parameters now support over 260 characters.
    - Added the ability to encode/decode a file using Base64 encoding by way of the new File System (Base64 encode/decode) activity.
    - The File System (Get information) activity now provides the ability to include checksums for all files.
    - The File System (Dataset to CSV) activity now supports enclosing dataset cell values in double quotes (") in CSV files.
    - Improved the performance of the File System (Dataset to CSV) activity.
- Terminal Action Enhancements
    - Added the ability to select the terminal window resolution for TN3270 and TN5250 emulations to the Terminal (Connect) activity.
    - Added the ability to attempt to automatically signoff from a terminal before disconnecting for TN3270 and TN5250 emulations to the Terminal (Connect) activity.
    - Added the ability to change font sizes for TN3270 and TN5250 emulations to the Terminal (Connect) activity.
    - Terminal - Connect activity supports public key authentication method.
- Image Action Enhancements
    - The Image action now supports .tif and .jpeg file formats.

- Compression Action Enhancements
  - Added the ability to verify if compressed files are valid and not corrupted by way of the new Compression (Verify) activity.
- HTTP Action Enhancements
  - Added the ability to modify existing data or a file on the specified server by way of the new HTTP (Patch) activity.
  - The HTTP (Post) activity now provides the ability to submit HTTP Post requests that do not contain a body.
  - The HTTP (Get) activity now accepts the "Create and Populate Dataset" field as a valid action output without an associated variable or output file.
  - Added the ability to create predefined HTTP connections using the new HTTP (Define) activity. Users can define HTTP connection and authentication information in a single place and then reuse it through a task in various HTTP steps.
  - Added support for additional authentication means (OATH 2.0, Bearer Token, API Key).
  - Corrected numerous issues involving JSON decoding.
- Exchange Action Enhancements
  - Added support for Exchange Online with Modern Authorization to the Email Server Settings.
  - Added support for Exchange Online with Modern Authorization to the Email Default Task Agent Properties.
  - Added support for Exchange Online with Modern Authorization to the Email Default Properties.
  - The hot key for each Exchange activity is now unique.
  - The Exchange (Get object(s)) activity now returns an empty dataset and no longer fails if no objects exist.
  - The Exchange Action as well as all other Actions and Automate/Enterprise components that employ exchange functionality have been updated to support TLS 1.2.
- PDF Action Enhancements
  - Added the ability for the PDF (Insert) activity to perform an insert at the last page of a PDF document.
  - Added new annotation management activities (Add annotation, Delete annotation(s), and List annotation(s)).
  - Added the ability to insert an image as a new page in a PDF in the PDF (Insert) activity.
  - Corrected numerous issues with the PDF action.

    - The PDF (Get attachment(s)) activity now provides the option to overwrite existing file attachments with the same name or individually save them with unique file names.
    - The PDF (Extract) activity now provides the option to extract contents into a single, multi-page TIFF file.
    - The PDF (Create) activity now provides the option to change page orientation.
- Email Action Enhancements
    - The Email (Send Message) activity can now create a dataset to capture information regarding each email sent.
- Dialog Action Enhancements
    - The Dialog (Open File) activity now provides improved file and folder browsing navigation.
- BASIC Script Action Enhancements
    - The BASIC Script (Execute) activity's Embedded text box has been increased in size.
- Web Service Action Enhancements
    - Web Service action has been updated to support TLS 1.2.

Installing the Advanced Workflow Module

The Advanced Workflow module (AWM) is installed with Fortra's EFT Server and is included in the 15-day trial of EFT, during which you can create, edit, and execute powerful workflows using the EFT Event Rule system. After the trial has expired, you can still create new workflows and edit existing ones; however, after the trial expires, you will no longer be able to execute the workflows with EFT Event Rules. After you purchase and activate a serial numberfor the module, you will once again be able to use the workflows in Event Rules. The workflows are not deleted until you delete them.

EFT subscription licenses have a week-long grace period in which the module will continue to function after being expired. Automate does not have this week-long grace period. When the Advanced Workflow module (AWM) expires from a subscription license and enters its grace period, the Automate side will expire with no grace period; the AWM module will stop functioning in its grace period.

IMPORTANT: If you are upgrading from a version of EFT before v8.2, please read Upgrading the Advanced Workflow Module. There are numerous items that you need to know BEFORE you upgrade, such as the conversion of Advanced Workflow AML files.

Upgrading the Advanced Workflow Module

The Advanced Workflow module (AWM) is installed with Fortra's EFT Server and is included in the 15-day trial of EFT, during which you can create, edit, and execute powerful workflows using the EFT Event Rule system.

> **NOTE:** If you are not upgrading from an earlier version of EFT/AWE, please refer to Installing the Advanced Workflow Module and Installing the Server, Interface, and Modules.

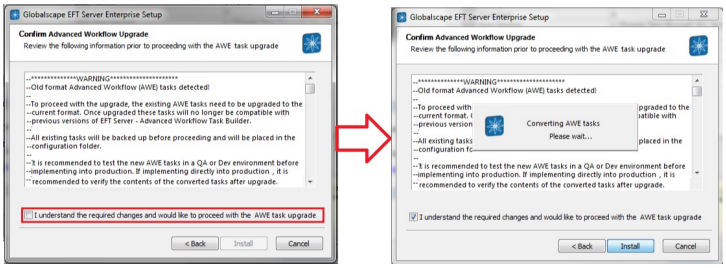
Important information to know before upgrading EFT v8.2:

1. EFT is compatible with latest version of Automate 2024.
2. Automate 2024 will not support AWE 10 and, as a result, is not backwards compatible. You can use your AML files but they must be converted to the new version. If your AMLs are in the default folder, they will be upgraded automatically. If they are in a remote folder, you will have to convert them manually. (See how below.)
3. If you are upgrading from an earlier version of EFT, the EFT installer will upgrade Fortra's Automate v10 to Fortra's Automate 2024.
4. Automate installation with EFT ***cannot*** be skipped and will be automatically upgraded.
5. If you attempt to install EFT on a system that contains a standalone version of Automate, the standalone version of Automate must be later than the bundled version of Automate in the EFT installer.

   For example, if the EFT installer includes Automate v24.1.1.8, then the version installed on the system must be v24.1.1.8 or later. If the version on the system is earlier, such as v24.1.0.22, the EFT installer will not proceed with installation.

6. Automate requires Microsoft .NET 4.8 for new installations or upgrades to complete successfully.
   - If .NET 4.8 is missing, you will receive a prompt related to this requirement during a new installation or an upgrade.
   - .NET 4.8 is core is included in Windows Server 2022 and, as a result, EFT v8.2 will install without any prompts.
7. During upgrade to EFT 8.2, as the EFT service is starting, EFT will trigger **an import utility that will convert all the AML tasks from version 10 to version 2024**. You might notice a bit of a spike in CPU, and it might take a few minutes for the conversion to complete.

8. If v8 or v10 AWE files are detected upon upgrade (in <config location>/AWE folder/SQLite database) the EFT installer should prompt you to perform .aml conversion manually. External AML (Automated Markup Language) files located outside of EFT will not be included in the backup/upgrade process. You will have to upgrade them manually. (386924) (See NOTE below.)
    a. You are presented with a dialog box showing information related to the Advanced Workflow upgrade:



    b. Select the check box at the bottom of the dialog box confirming that you understand the changes.
    c. Click **Install**. (Install is only available after you select the check box.)
9. If an AML file has extra characters that do not appear to belong there (such as "aaaaaa<AMTASK>") or if parts of steps are missing, the upgrade will fail and you will have to remove the extra characters and manually convert the file.
10. On upgrades, before performing the conversion process, EFT will create a backup folder in the EFT config location and make a copy of any existing older-format .aml files or create a copy of the SQLite Advanced Workflow database, if available.
11. If the upgrade process fails, EFT will create an Advanced Workflow migration log file with information about conversion process so that the admin can be aware of any issues or changes detected during conversion.

    After EFT completes the upgrade to EFT v8.2, Advanced Workflow module v10 will be upgraded to Automate 2024.

12. There is no customization option available for Advanced Workflows (other than Task Builder color/font options.)
13. Actions that require user interface interaction will not run when triggered via EFT event rules, as EFT actions run unattended.
14. The EFT installer will not provide a choice whether to install or not install the Automate software that is bundled with EFT. However, if the EFT installer detects there is already a standalone Automate Desktop installed, EFT will skip the installation of the bundled version. In any scenario, the Start menu will contain the Automate Desktop 2024 items.

The Advanced Workflow module has a 15-day trial. Try it out for 15 days; if you don't register it, you will not be charged for it. The Advanced Workflow module is registered in the EFT administration interface. Please refer Activating the Software for details.

To manually convert a file

> **NOTE:** Manually "updating" the AML files involves changing the version number at the top of the AML file in the `<TaskInfo>` section.
> **Change example:**
> ```
>  <AMTASKHEAD>
> <TASKINFO TASKVERSION="10.7.100.1" />
> </AMTASKHEAD>
> ```
> **to the new version** (*match the versions in the newly installed AML files*):
> ```
> <TaskInfo>
> <Version TaskVersion="24.6.1.22" MinVersion="0.0.0.0"
> AMLVersion="3.0" />
> </TaskInfo>
> ```

Advanced Properties for Advanced Workflows

If you have installed a stand-alone version of Automate, add the following advanced properties to the **AdvancedProperties.json** file in ..**\Program Data\Globalscape\EFT Server**.

- **AutomateInstallDir**
  - Automate installation directory; default is EFT installation folder.

    Any slash \ must be escaped in the path, as in C:\\Program Files\\Globalscape\\Automate\\
- **AutomateServiceName**
  - Type: string; "AutomateDesktop2024"

    The version number used in AutomateServiceName is subject to change and should be updated according to the version you have running on your system. For EFT 8.2, we support Automate Desktop 2024; however, when the next version of Automate is released, the Advanced Properties file should be updated accordingly.
- **AutomateRestApiPort**
  - Type: number; range [10000, 12000]; default is 11012.

The EFT logger will not display advanced properties that are using default values, such as when the port using the default value of 11012; if you changed this to a non-default value, you would see a log entry.

NOTE:

```
{
       "AutomateInstallDir":"C:\\Program
Files\\Globalscape\\Automate\\",
       "AutomateServiceName":"AutomateDesktop2024",
       "AutomateRestApiPort":11012
}
```

- Refer to Advanced Properties for more information about advanced properties.
- After adding or editing the advanced properties file, close the EFT administration interface, restart the EFT server service, and then reopen the interface.
- Make sure all the paths are specified correctly.
- Restart the EFT service after you save the changes.

AML-related issues when upgrading to Automate 2024:

- **Issue**: SFTP connections failing in Automate 2024 after upgrading to 8.2.0.46.
  - **Solution**: Automate SFTP action is using KEX algorithms disabled/ not supported in EFT. Refer to SFTP-connections-failing-in-Automate-2024-after-upgrading for more information.
- **Issue**: An event rule running an Automate Workflow task that contains Display Dialogs: the dialog will pop up on user's screen every time the event rule is triggered on a given schedule.
  - **Solution**: The Dialogs (popup expecting an interactive user action) within the AML should be replaced with an appropriate alternative (Windows Event Logs, Automate variable preset).
- **Issue**: "Query a CSV file" sample: If upgraded from an older version, running the task will fail with an error stating the issue with Connection provider.
  - **Solution**: Provider should be set to "Microsoft.ACE.OLEDB.16.0", which would require the user to install "Microsoft Access Database Engine 2016 x64" on the system if it's missing. The provider should be installed when using this action.
- **Issue**: AML containing "Web Browser" action, will show up as "Step contains error" when upgraded from older versions, as this action will no longer be available.

    - **Solution**: User should manually fix it by his preferable way.
- **Issue**: AML containing DaysInMonth(07) format used will not work in new version of Automate.
    - Solution: User should manually replace it with new supported alternative: DaysInMonth(dateexpr), DaysInMonth(Now()), DaysInMonth(DateAdd ("m",1, Now())), DaysInMonth(DateSerial(2004,02,34), etc. See Automate help documentation.
- **Issue**: Some AMLs will have lots of redundant spaces on indented lines.
    - **Solution**: This is only cosmetic and does not affect the performance of the step.
- **Issue**: Some AMLs could have extra characters that do not appear to belong there (such as "aaaaaa<AMTASK>") or parts of steps are missing, and the upgrade will fail.
    - **Solution**: Remove the extra characters and manually convert the file.
- **Issue**: Using an array or dataset to store into a variable will cause the Automate task to fail.
    - **Solution**: Use VBScript to assign a value (that is not a simple type) to a variable or to iterate over the array and copy the elements to the target array.

Automate Service Account

The Automate Desktop service (also known as the Task Service, AMTS.exe) enables tasks created using Automate Desktop to trigger automatically on the computer. If this service is stopped, Automate Desktop tasks will not be run at their scheduled times.

To continue to run EFT event rules when the Windows session is logged out or locked, or the EFT server service account is logged out, ensure that the *Automate Service Account* (described below) is enabled on the **Server > Administration** tab in the EFT administration interface.

> **NOTE:** EFT administrators should not modify the Automate Desktop 2024 service in the Microsoft Manage Console **Services** dialog ("Log on As") as this will break functionality. Refer to the Knowledgebase article #11645 Modifying the Automate Desktop 2024 service account breaks functionality for more details.

Before creating or using Advanced Workflows in EFT, you should wait a while after any of the following actions have occurred:

- When an EFT site is getting started (every time a site is started), it sets the Automate license and triggers an Automate service restart. Therefore, after a site is started, don't immediately open any Advanced Workflow tasks or Event Rules containing Advanced Workflows. It simply won't work, because it might be that the Automate service has not yet started, because this may take some time.
- Any changes to an EFT license, extending or deregistering the trial, or registering or deregistering the Advanced Workflows module will set the Automate license expiration dates accordingly and trigger Automate Service restart. Meaning that after any of those actions, you may have to wait until the Automate service gets started.
- Automate service is started or restarted in each of the cases described above and on EFT site start.
- Automate service is started or restarted when an Event rule is triggered, but for some reason Automate service shows it has stopped. Then EFT restarts it and then re-triggers the Event rule.

The Automate service enables tasks created using the Task Builder to trigger automatically on the computer. If this service is stopped, tasks will not be run at their scheduled times. **The Task Builder requires a valid Windows user account to be**

enabled on the computer on which it is running to execute Advanced Workflows in event rules.

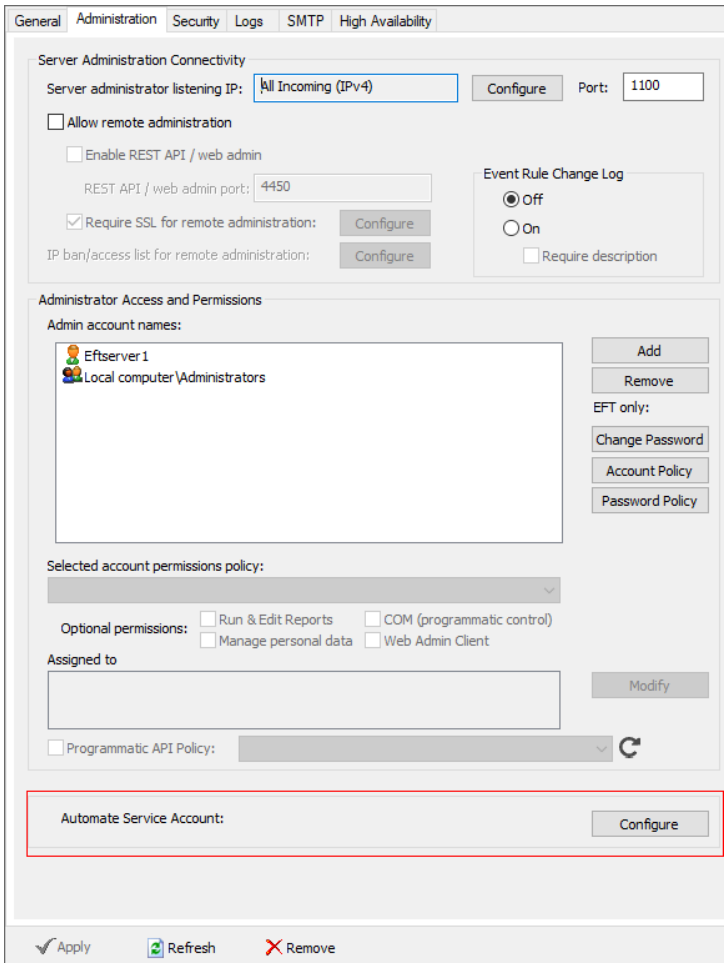
When the EFT administrator account or EFT service account has logged off of a Windows session, an *Automate service account* is needed to execute Advanced Workflows via event rules. EFT provides a way for the administrator to enter credentials for a Windows user account and persist them as part of EFT's configuration. The Automate Service account is enabled in the EFT administration interface on the **Server > Administration tab**.

For example, the AWM **Dialog** action requires user input, which is not desired since the EFT administration interface is not continuously monitored and a user prompt could delay the completion of event rules. You should enable the Automate Service Account in EFT to prevent the Dialog pop-up from occurring. Tasks will run in the background without popups.

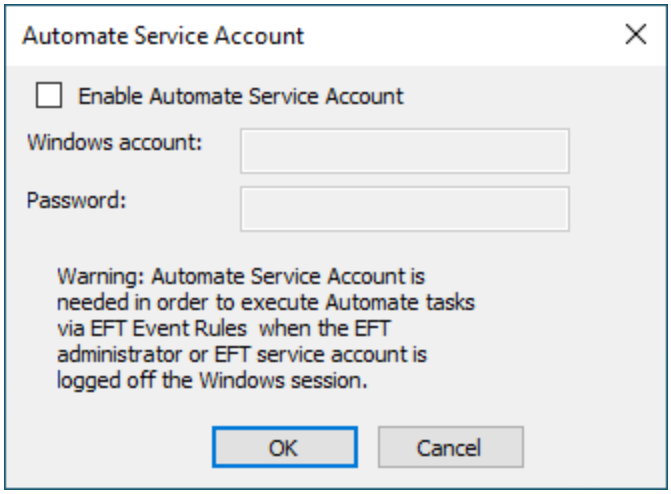
> **NOTE:** The Automate Service Account (in EFT) is a local system account and is not synchronized between clusters.

To enable the Automate Service Account

1. At the bottom of the **Server > Administration** tab, next to **Automate Service Account**, click **Configure**.



The **Automate Service Account** dialog box appears.



2. Select the **Enable Automate Service Account** check box.
3. Provide the **Windows account** name and **Password** to be used for the Automate service account.

> **NOTE:** The Automate Service Account is a local system account and is not synchronized between clusters.

4. Click **OK** to close the dialog box and then click **Apply** to save the changes.

   Tasks will run in the background without popups.

Introduction to Advanced Workflows

The Advanced Workflow module adds additional automation capabilities to the EFT Event Rules system, allowing you to add scripting and variables to *Workflow Tasks*, then add these reusable Workflows to Event Rules. A Workflow is a series of steps that can perform file transfers, batch data processing, application testing, and so on, and are defined to run automatically when started by some event. The Advanced Workflow module is built on components of the Automate Desktop product from Fortra. EFT Event Rules use the Automate Task Builder and Actions, but not the Automate Task Administrator. Instead of the Automate Task Administrator, events and triggers are managed by the EFT Event Rules system.

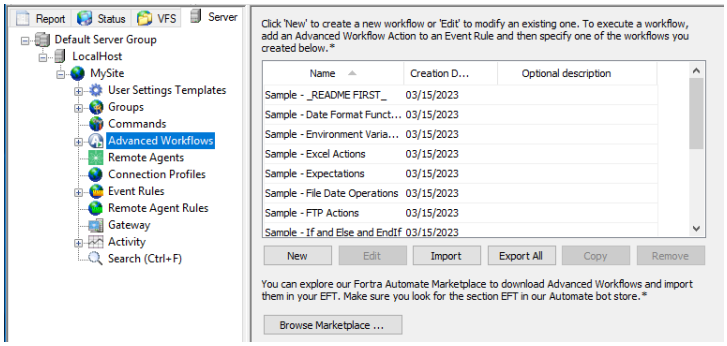
> **NOTE:** Both Automate Desktop Task Administrator and Automate Desktop Task Builder are installed with EFT. However, Automate 2024 will only work in EFT if the Advanced Workflow module is licensed in EFT (Help > About). The Automate Desktop service only starts when EFT triggers an event rule that uses Automate actions.

Some Automate actions are hidden by default from the list of available actions in the Advanced Workflow Task Builder. In many cases, these hidden actions are simply not applicable to the environment in which Advanced Workflows run, such as those geared around interactive desktop use cases or actions in which the Automate functionality is simply not carried over to the Advanced Workflow implementation in EFT (such as Twitter, Speech, and Multimedia actions). In other cases, such as for AS2 and Automate Schedule, they conflict with EFT modules. To find available Advanced Workflow module actions and descriptions that can be used in EFT Event Rules, refer to the Available Actions.

You can create your own workflows from the Advanced Workflows node in EFT or, in Automate 2024, get a few sample workflows from the Automate Connector Hub (Internet access required).

To go to the Automate Connector Hub

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Advanced Workflows** node.
3. In the right pane, the **Advanced Workflows** tab appears.



4. In the right pane, click **Browse Marketplace**. The default browser opens to the Automation Connector Hub.
5. Scroll down on the page to browse all of the connectors.

Automation Connector Hub offers pre-built workflows, that you can download and import into EFT event rules. The Hub has numerous Automate tasks (Workflows) for applications from Active Directory to Zendesk. Click the link for the workflow that you are interested in. The linked page provides a description of the workflow and a link to download it. You can download multiple workflows at a time. There are more than 200 free workflows and about 15 "premium" workflows.

For details of specific Automate actions, please refer to the Automate Task Builder help inside EFT.

Workflow Concepts

The fundamental concept of Advanced Workflows is the automation of front and back-office business processes. Advanced Workflows is a software platform for building, managing, and launching automated tasks within EFT Event Rules. Tasks are developed via drag-and-drop without writing a single line of code. Simply drag together each action object in the sequence it should be executed.

Architecture

Advanced Workflows breaks down business processes into "visual" steps with the use of "actions." Multiple steps combined together are called a "task." Actions are used to instruct Advanced Workflows how to carry out a task. A "trigger" is a condition or event in Windows that essentially directs to execute a task automatically.

Task- The primary and most important object, a task is composed of a series of steps based on actions. Tasks can be designed to any of a very wide spectrum of business processes.

Actions - The available processes that can be used to build the steps to be carried out when a task is run. More than 300 actions are available from which to build tasks. These actions are assembled visually (without the use of code) via drag-and-drop in the Task Builder interface. Each action used to construct the task becomes a step. Upon execution, these steps are performed in a sequential order.

Components

The three main components are as follows:

Task Builder- Used to visually assemble actions into sequential task steps to be carried out. Additionally, the Task Builder is fully equipped with a wide variety of debugging tools to easily examine and troubleshoot problem tasks, eventually ensuring maximum reliability when the task is put into production.

EFT Event Rules - The central tool used to administer and customize all aspects of Advanced Workflows. EFT Event Rules organize tasks, connect to remote installations, and set task properties. In addition, it is used to administer global settings such as the default mail server, default logon properties, database connections, and much more.

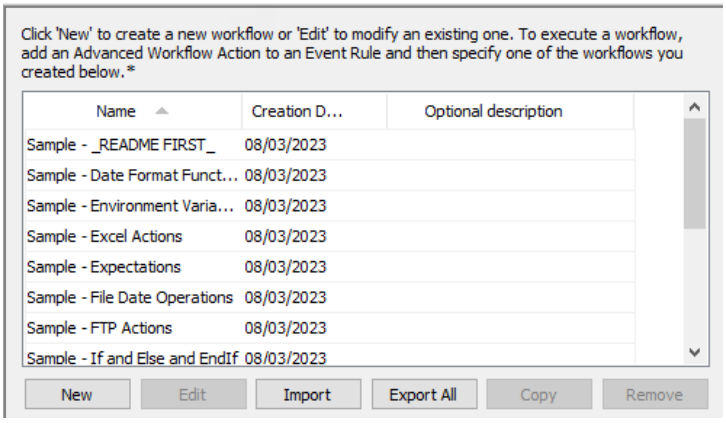
Advanced Workflow Action - Launches tasks according to the triggers attached to them.

The Workflow Task Builder Overview

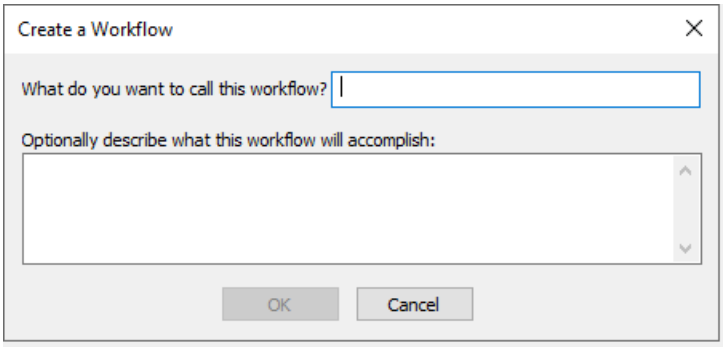
The Task Builder is used to create the workflow (Task) that you want to use as an event rule Action.

To open the Task Builder

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Advanced Workflows** node.
3. In the right pane, the **Advanced Workflows** tab appears.

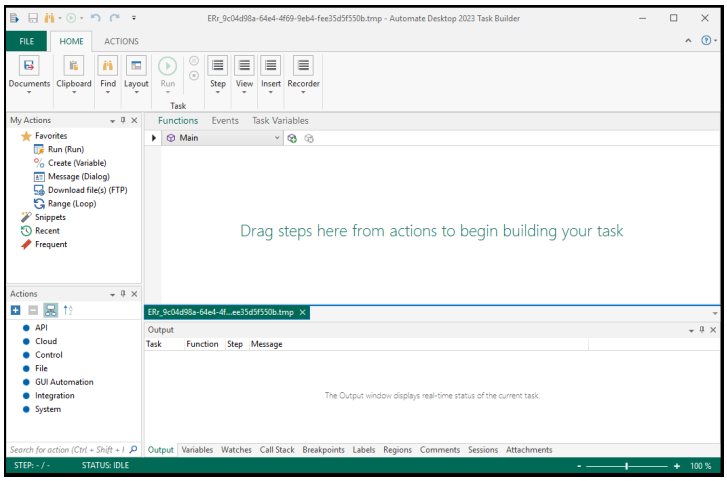


4. In the right pane, click **New**. The **Create a Workflow** dialog box appears.



5. In the **What do you want to call this workflow** box, specify a name for the Workflow, then click **OK**.

The Workflow **Task Builder** appears.

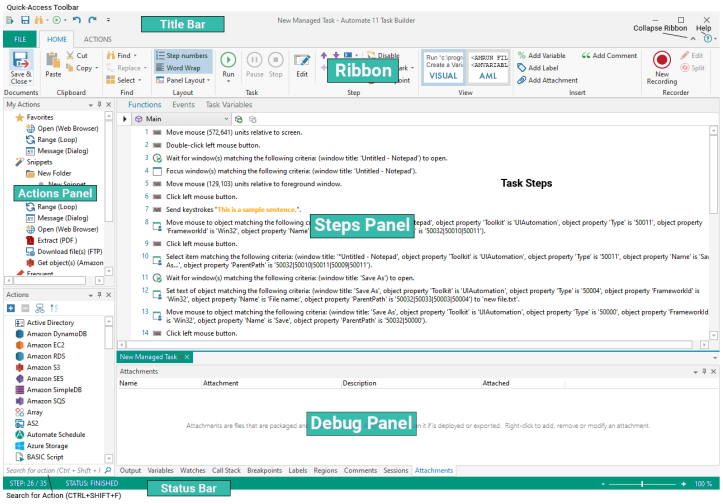


For details of how to create or edit workflows, refer to Creating Workflows for Use in an Event Rule.

Task Builder Interface

The Task Builder is an intuitive project designer used to visually assemble and test the activities that the task should carry out when it is executed (either manually or automatically by a trigger). Task steps are created by visually dragging-and-dropping Automate Desktop activities from an actions palette and placing them in the sequence desired for execution, eliminating the need to write code or create batch files. Additionally, the sequence of steps are described in plain English and presented in a way that clearly describes what they do.

The Task Builder includes a variety of testing and debugging features that displays verbose, real time data about a task, which aids the administrator in monitoring and debugging tasks as they are being constructed. This ensures that newly created tasks are functioning properly before they are put into production. For instance, the administrator can perform a series of “test runs” within the Task Builder and use a variety of intuitive debugging and diagnostic features to determine the cause of failing or problematic tasks.



The Task Builder interface is comprised of several panels or window panes. The table below lists each (in alphabetical order) along with a description.

Section	Description
My Actions	The **My Actions** panel saves a list of your favorite, recently used, and mostly used activities, and allows creation of snippets, which are copies of specific steps that contain predefined properties and settings.
Actions Panel	The **Actions panel** encompasses all of the actions available to construct the steps of a task.
Debug Panel	The **Debug** panel contains several views that are separated by tabs. Each view is comprised of a different debug tool. A different pop-up menu will appear for each view displaying the options available for that particular debug tool.
Ribbon	The **Ribbon** spans the top of the Task Builder, directly below the title bar. It is filled with graphical representations of control elements that are grouped by different functionality. Commands are organized in logical groups, which are collected together under operation related tabs.
Status Bar	The **Status Bar** is located at the bottom of the Task Builder and displays real-time progress of a running task through graphics and text.
Steps Panel	The **Steps** panel displays the actions and activities selected from the **Actions** Panel that will be carried out when the task executes.

To find available Advanced Workflow module actions and descriptions that can be used in EFT Event Rules, refer to the Actions panel in the Task Builder accessed from the EFT administration interface.

For details of specific Automate actions, please refer to the help in the Task Builder interface, or go open **..\Program Files\Globalscape\AutoMate\Help\Content\Task_Builder\Actions_Activities**.

Adding Task Steps

Once in the Task Builder, task construction can start by dragging the desired action from the Available Actions pane onto the Steps panel (as shown below). Doing so will open a properties dialog box for that action where parameters and specifications can be defined. Each type of action has its own set of properties. Specific actions may contain multiple activities to select from. Choosing the desired activity will populate the dialog with the proper properties and settings of that activity.

To add steps

1. In the Actions panel of the Task Builder, find the action/activity you want to add. You can find an action by clicking the plus signs (**+**) on any of the categorized folders, or by entering the name of the action or activity in the **Search for action** box at the foot of the Actions panel. When you use the **Search for action** box, the actions list is filtered as you type to include only those actions / activities that contain a match for the entered text (see Finding Actions for more details).
2. Drag the action / activity into the **Steps** panel (as shown below) or simply double-click the action / activity.

   The properties dialog box for that action opens.
3. Enter properties and click **OK**. The action / activity then becomes a step in your task. Repeat this process to add additional steps in sequence.
4. If you need to change the sequence of the steps, select the step you want to move and use the arrow buttons on the toolbar to move it up or down (for further information, see Editing Task Steps).
5. If you need to delete a step, right-click it, and select **Delete**.
6. When you are finished adding steps, click **Run**to test the task.
7. To save without closing Task Builder, from the Quick Access Toolbar (located above the ribbon by default), click the **Save** button or press CTRL+S.
8. To save and close Task Builder, from the ribbon, click the **Save and Close** button.
9. To save to a separate location, from the ribbon, select **File** > **Save Copy As** and navigate to the location in which to save your copy.

> **NOTE:** Unlicensed actions and activities will appear opaque in the Actions panel. Double-clicking, dragging or trying to add them to the Steps panel in any other way will generate an error.

Using add / insert option

- The Ribbon's **Actions** command group contains commands that can be used to add or insert a step.

To add an action as the last step

1. In the **Actions** panel, select the action / activity to add.
2. Click **Add Step**from the ribbon.

To insert an action in between steps

1. In the **Actions** panel, select the action / activity to insert.
2. In the **Steps** panel, select the step that you want the new action / activity to be inserted.
3. Click **Insert Step** from the ribbon. The new action will be inserted directly below the step you selected.

> **NOTE:** To add steps from the Recent, Frequent, Favorites, or Snippets folder, see My Actions Panel.

Editing Task Steps

Along with the ability to edit the Propertiesof individual task steps, many adjustments can be performed on any step once they are added to the Task Builder's Steps panel. You can move, indent, disable or delete one or more existing steps. You can perform cut, copy, and paste commands as well.

Commands are conveniently located on the Ribbonor by way of a context menu that appears when right-clicking a specific element. Certain ribbon commands become active only when items they apply to are selected, making it easier for you to distinguish relevant commands and avoid selection of unrelated ones.

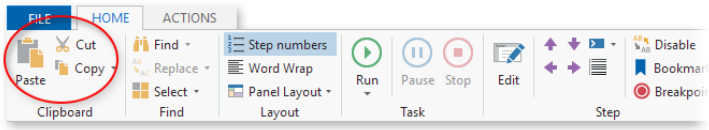
The Quick Access Toolbar contains **Undo**and **Redo** commands that apply to all edit operations allowing you to undo one or more incremental sequence of changes in case you make a mistake or redo them in case you change your mind.

Editing Step Properties

The properties of any task step can be easily viewed or modified once it is added to Task Builder's **Steps** panel. For convenience, step properties can be accessed in various ways.

To view or modify the properties of a step

1. In the **Steps** panel of Task Builder, select the step that contains the properties you wish to modify and double-click on the step.
2. Perform the desired changes in the properties dialog that appears, and then click **OK** to save changes.



Moving Steps

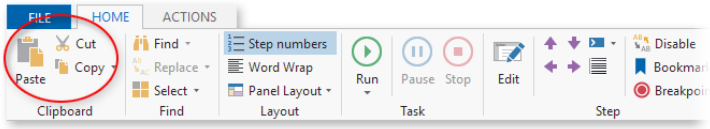
Steps can be moved freely within the Steps panel. You can modify the sequence at which steps execute by moving them above or below other steps. Task Builder supports movement of multiple sequenced steps (for example, steps 3, 4, and 5) as well as multiple non-sequenced steps (for example, steps 3, 6 and 8). For convenience, such operations can be performed in various ways.

To move steps using the Move Up or Move Down commands

1. In the **Steps** panel of the Task Builder, select the steps you want to move up or down the step sequence. To select more than one step, hold down CTRL during selection.
2. From the ribbon, click the **Move Up** or **Move Down** arrow. Each click is equivalent to a single line of movement.

To move steps using Cut and Paste commands

1. In the **Steps** panel of Task Builder, select the steps you want to move up or down the step sequence. To select more than one step, hold down CTRL during selection.
2. From the ribbon, click **Cut** (you can also use CTRL+X) .
3. Select a desired location in the **Steps** panel and click **Paste**from the ribbon (you can also use CTRL+V).



To move steps using Drag & Drop actions

1. In the **Steps** panel of Task Builder, select the steps you want to move up or down the step sequence. To select specific steps or a block of steps, hold down CTRL during selection.
2. Hold down the left mouse button while dragging the highlighted steps to the desired location, then release the mouse button to complete the operation.

Indenting Steps

You can increase or decrease indentation of one or more steps as a way to organize your steps. Task Builder supports indentation of multiple sequenced steps (for example, steps 3, 4 and 5) as well as multiple non-sequenced steps (for example, steps 3, 6 and 8).

To increase or decrease indentation

1. In the **Steps** panel of Task Builder, select the steps to increase or decrease their current indentation. To select a block of sequenced steps or specific non-sequenced steps, hold down CTRL during selection.
2. To increase indentation, click the arrow pointing right in the ribbon's **Step** command group (you can also use CTRL+ right arrow key). To decrease indentation on an indented step, click the arrow pointing left (you can also use CTRL + left arrow key).

> **NOTE:** Left justification of an indented step is based on the parent step (if relevant) and the default indentation settings applied by way of Task Builder **Options > Formatting**.

To reset indentation

1. In the **Steps** panel of the Task Builder, select the steps that should be reverted back to their original indentation level. To select a block of sequenced steps or specific non-sequenced steps, hold down CTRL during selection.
2. From the ribbon, click the **Reset Indent**. Hold down the left mouse button while dragging the highlighted steps to the desired location, then release the mouse button to complete the operation.

You can reset one or more steps to their default indentation level. From the ribbon's **Step** command group, click the **Format Steps**command. This enables or disables auto-formatting of steps. When enabled, blocks of steps contained within a conditional (If) statement or Loop process are formatted (indented) to improve distinction (this command is enabled by default).

Disabling, Enabling, or Deleting Task Steps

Steps of a task can be disabled or re-enabled to use or test different versions of the same task. The **Disable**button on the ribbon or context menu acts as a toggle to disable an enabled step or re-enable a disabled step. When a step is disabled, it is grayed out by default in the **Steps** panel and it is treated as a comment and ignored when the task runs.

To disable or enable a task step

1. In the **Steps** panel of the Task Builder, select the steps you want to disable. To select more than one step, hold down CTRL during selection.
2. Click the **Disable** button on the ribbon under the Home tab (you can also right-click on the steps, and then click **Disable**).

> **NOTE:** To re-enable, follow the same instructions.

To delete a task step

1. In the **Steps** panel, select the step or steps you wish to delete. To select more than one step, hold down CTRL during selection.
2. Right-click on your selection, and then click **Delete** (you can also use the Delete key).

Step Numbers & Word Wrap

By default, the **Steps** panel displays numbers to represent each step in the task are displayed for each step in the Task Builder's **Steps**panel along with an icon designating the type of action used. Also the text (or AML code) that appears in this panel is word wrapped by default allowing all text to be visible in the window regardless of its size. Nonetheless, these options can be customized according to each user's preference.

To turn Word Wrap on or off

1. From the Ribbon, click **Home**.
2. From the **Layout**command group, click the **Word Wrap** button to toggle Word Wrap on/off.

To disable or enable step numbers

1. From the Ribbon, click **Home**.
2. From the **Layout**command group, click **Step numbers** to toggle step numbers on/off (also shown below).

Switching from Visual to the AML View

The Task Builder offers two ways in which to view the steps of a task. The default appearance displays a plain-English, easy to comprehend text description of each step. They can also be displayed in AML (Automate Desktop Markup Language) format, which is the internal program language encompassed in Automate Desktop. When set to this view, those who understand AML can edit their code directly from the Task Builder's Steps panelor copy the code onto an external text editor such as Notepad.

To switch from Plain Text to AML or AML to Plain Text

1. From the Ribbon, click **Home**.
2. In the **View**command group, select **AML**to switch to AML code view or **Visual**to switch to plain text view.

To edit code in the AML view

1. In the **Steps** panel, select the step to edit.
2. Click the step again to make the code editable.
3. Make the desired changes.

Undoing and Redoing Changes

To enable task development to be as simple and painless as possible, an **Undo** and **Redo** command is included on the Quick Access Toolbar. Undo reverses the last action you performed, and Redo undoes the last Undo action, in case you change your mind. Task Builder keeps track of all previously performed actions, therefore, you can reverse the actions you performed one action at a time, in reverse consecutive order, up to and including the first action.

To undo changes

- Click the **Undo**command on the Quick Access Toolbar or press CTRL + Z. Undo reverses the last editing action. If you delete one or more steps, you can use **Undo** to restore them and all their properties. You can perform as many Undo actions as you like.

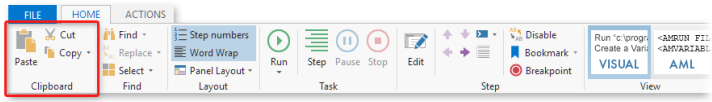
To redo a change after an undo

- Click the **Redo**command on the Quick Access Toolbar or press CTRL + Y. This restores the last action you performed if no other actions have occurred since the last Undo. The **Redo**button is normally inactive and becomes active only if an **Undo** is performed.

Copying and Reusing Task Steps

The reuse of code is a common technique In computer programming, used to save time, reduce redundancy and eliminate errors by applying the same segment of code in multiple applications. The Task Builder plays a similar role by allowing task steps to be copied and re-used within the same task or across multiple tasks. This article describes various methods to perform this operation.

The **Home** tab of the ribbon contains clipboard commands that allow you to reuse steps within a task by copying one or more steps and pasting them onto another section of the task. Because more than one instance of Task Builder can be opened simultaneously, code reuse can be performed across multiple tasks as well. The **Copy** command, in effect, copies the .AML code associated to each task step. This code can be pasted onto a specific step on the same task or another task using the **Paste** command. Alternatively, a **Copy > Description** command is available, allowing the textual description of each step to be copied and pasted onto another application outside of Task Builder, such as an email message or text file.



To copy and paste steps in the same task

1. Select the task you want to work with to open Task Builder.
2. From the Steps panel, select the steps you wish to copy. To select a group of steps, hold down CTRL during selection. Use CTRL+A to select all.
3. On the ribbon, select the **Home**tab and click the **Copy** button from the Clipboard command group. Or, right-click the highlighted steps and select **Copy** from the context menu.
4. From the Steps panel, select the step you want to place the previously copied steps. Then, on the ribbon, select the **Home** tab and then click the **Paste** button from the Clipboard command group.

The copied steps are pasted precisely at the step you selected. Existing steps are moved directly below the pasted steps.

To copy steps from one task to another existing task

1. Select the task you want to copy steps from in order to open the first instance of Task Builder.
2. Select the task you want steps to be pasted onto in order to open the second instance of Task Builder.

3. From the Steps panel in the first instance of Task Builder, select the steps you wish to copy . To select a group of steps, hold down CTRL during selection. Use CTRL+A to select all.
4. On the ribbon, select the **Home**tab and then click the **Copy** button from the Clipboard command group.
5. From the Steps panel of the second instance of Task Builder (the one you wish to paste steps onto), on the ribbon, select the **Home** tab and then click the **Paste** button from the Clipboard command group.

The copied steps are pasted precisely at the step you selected. Existing steps are moved directly below the pasted steps.

To copy steps from one task to a new task

1. Create and edit a new task to open an instance of Task Builder.
2. Select the existing task you want to copy steps from to open another instance of Task Builder.
3. From the Task Builder's Steps panel of the existing task, select the steps you wish to copy . To select a group of steps, hold down CTRL during selection. Use CTRL+A to select all.
4. On the ribbon, select the **Home**tab and click the **Copy** button from the Clipboard command group.
5. Select the Task Builder instance associated to the new task.
6. Right-click anywhere inside the empty Steps panel and select **Paste** from the context menu. The copied steps are pasted directly onto the Steps panel of the new task.

To copy and paste step descriptions

1. From the Steps panel of Task Builder, select the steps in which to copy the description from. To select more than one step, hold down CTRL during selection or use CTRL+A to select all steps.
2. From the ribbon interface, select **Copy > Description** from the **Clipboard** command group or right-click and select **Copy > Description** from the context menu.
3. The text can be pasted into any Automate Desktop field or text-box where plain text is accepted. You can also paste copied steps or step descriptions in other documents such as email messages or text files.

NOTE:

- When **Copy** > **Description** is selected, the content of the clipboard becomes populated with the “Visual View” text-only description that is normally displayed in the Steps panel and does not contain any AML code (even if the Steps panel is currently set to be viewed in AML format).
- To copy the AML code of a particular step instead of the text description, select **Copy**from the ribbon interface or right-click the step and select **Copy** from the context menu (not **Copy** > **Description**). Doing so will allow you to paste the AML code into a document, text file or any field in Automate Desktop that accepts text.
- Selecting **Copy** will also allow you to paste the content as a step in the Steps panel.

Steps of an existing task can be re-used in a newly created task by selecting the **Save Copy As** command. This is an ideal method for copying all of the steps of an existing task onto a new task.

To save a copy of a task

1. Open the task you wish to copy steps from by doing one of the following:
    - From Task Administrator, right-click the task and select **Steps**. The Task Builder appears for this task.
    - Select the task from the Repository section of the Server Management Console or Workflow Designer. A separate instance of the Task Builder appears for each task.
    - If a new (unmanaged) task was initially created by directly opening the Task Builder from the Start menu, select **Open**from the Application menu and navigate to the task (.AML) file you wish to open and click the **Open** button. In this case, a separate tab appears in the Steps pane of the Task Builder, each signifying an open task.
2. From Task Builder's ribbon interface, select **File** > **Save copy as**.
3. Navigate to the desired location, enter a name for the new task, and click **Save**.

Using Snippets

Another way of using a group of steps within a specific task is to save the steps as Snippets. Snippets provide an easy way to implement frequently used code into a task. They are particularly useful to those who use specific activities that contain commonly used properties or settings. Instead of re-entering the properties for a specific activity or series of activities every time they're added as task steps, users can save existing steps as a snippet and simply drag and drop the snippet wherever it is needed in any task.

Finding and Replacing Text in Task Steps

Task Builder encompasses a comprehensive Find and Replace feature that enables you to search for every occurrence of a particular word or phrase in one or more open tasks, and optionally, replace them with the specified text. You can scope searches to the current task, current function, selected steps or all open tasks. Options and rules that you set can restrict the results to those that meet the criteria that you specify. For example, you can specify what direction you want to search or require that only text that matches the case of the text you entered should be found.

The **Find** and **Replace**controls are located in Task Builder's ribbon under the **Home**tab. To determine related hot-keys, hover your cursor over each control.

Finding text

The Find dialog searches through the AML code of the selected step or function, current task, or all open tasks (depending on the search options you choose). When finding one instance of text at a time, clicking **Find**highlights the next instance of text found.

To find text in one or more steps/tasks

1. In the Steps panel, click the step from which you want to start the search or specific steps you want to include in the search. To select more than one step, hold down CTRL during selection.
2. From Task Builder's ribbon, select the **Home**tab and click **Find** or press **CTRL + F**. The Find dialog appears.
3. In the Find dialog, do the following:

Use this...	To do this...
Look in	Select the scope of the search: • **Current task** - Search the AML of the current task. • **Current function** - Search the current function. • **Selected steps** - Search only the selected steps. • **All open tasks** - Search all tasks open in the Task Builder. The Task Builder application (AMTB.exe) must be opened directly in order for it to display multiple tasks. If it is opened by way of a managed task, then
Find what	Type the text you want to search for.
Match case	Find text only if it matches the case of the text you typed.

Use this...	To do this...
Match whole words	Find text only if it matches the whole word you typed.
Regular expression	Use regular expressions (notations for patterns of text) rather than the literal character. For more information, see **Regular expressions for finding text** below.
Search up	Searches will be performed from the bottom to the top.
Wrap searches	Automate Desktop will search for the specified text beginning at the point in the document where you are currently positioned, and will continue past the end, to the beginning of the document back to your current position. In other words, wrap search will search the entire document irrespective of where you may be positioned within it

4. Click **Find** . The found text (if any) is highlighted in the task.
5. Repeat clicking **Find** to find additional instances of the text.
6. Click **Close** when finished.

> **NOTE:** You can close the **Find** dialog and still find the next instance by clicking **Find Next** on the ribbon.

Replacing text

You can automatically replace text using the **Replace** dialog. This dialog has the same functionality as **Find**but allows you to make text substitutions in the current function, steps or tasks as shown below.

To replace text in a task

1. From the Task Builder ribbon, select the **Home**tab and click **Replace**. This opens the **Replace**dialog
2. In the **Replace** dialog, do one of the following:

Use this...	To do this...
Look in	Select the scope of the search: • **Current task** - Search and replace text from the AML of the current task. • **Current function** - Search and replace text found in the current function. • **Selected steps** - Search and replace text from the selected task steps. • **All open tasks** - Search and replace text within all open tasks in the Task Builder. The Task Builder application (AMTB.exe) must be opened directly in order for it to display multiple tasks. If it is opened by way of a managed task, then
Find what	Type the text you want to search for.
Replace with	Type the text you want to replace the original text with.
Match case	Find text only if it matches the case of the text you typed.
Match whole words	Find text only if it matches the whole word you typed.
Regular expression	Use regular expressions (notations for patterns of text) rather than the literal character. For more information, see **Regular expressions for finding text** below.
Search up	Searches will be performed from the bottom to the top.

3. Select one of the following:
    - To find one instance of the specified text at a time, click **Find Next**. The next instance is selected in the Steps panel in AML view. Repeat clicking **Find Next**to find additional instances of the text.
    - To replace the current text instance with the new text, click **Replace**.
    - To replace the ensuing text instance with the new text, click **Replace Next**. Repeat clicking **Replace Next** to replace additional instances with the new text.
    - To replace all instances of the specified text with the new text at the same time, click **Replace All**.
4. Click **Close**when finished.

Regular expressions for finding text

You can perform sophisticated find and replace operations in the Task Builder by using regular expressions. Regular expressions are useful when you do not know the

exact text or code you are looking for, or when you are looking for all occurrences of strings of text or code with one or more similarities.

A regular expression is a pattern of text that describes one or more variations of text or code that you want to find. A regular expression consists of specific characters, such as the letters **a**through **z** and special characters that describe the pattern of text, such as an asterisk**(*)**. For example, to find all variations of the word **page** in your task, you can enter **page*.** This finds all instances of **page**, **pages**, **pager**, and any other words that begin with **page**in your task.

When you use regular expressions in your searches, there are specific rules that control which combination of characters perform specific matches. Each regular expression or combination of regular expressions is referred to as syntax. You can use multiple regular expressions in one syntax to precisely target your search. The following table displays a list of common expression syntax and their description.

Syntax	Expression Description
.	Any character acts as a wild card to match any single printing or non-printing character with the exception of the newline (\n)character. For example, the regular expression c.t matches the strings cat, c t, cot, but not cost. In this example, the period (.) is a wild card for a single character. It appears between the letters 'c' and 't', so any single character between the characters 'c' and 't' will match the expression—even if it is a space.
*	Maximal — zero or more matches zero or more occurrences of a character that precede the expression, matching as many characters as possible. The regular expression .* matches zero or more occurrences of one character. For example, the regular expression b.*k matches book, back, black, blank, and buck. In this example, we combine the period (.) with the asterisk (*) to make one syntax. The period (.) appears immediately before the asterisk (*) expression. The asterisk (*) matches zero or more occurrences of any character between 'b and 'k'. The period (.) acts as a wild card for the characters between 'b' and 'k'. In this example, it means that any character between 'b' and 'k' can be repeated.

Syntax	Expression Description
+	Maximal — one or more matches one or more occurrences of a character that precede the expression, matching as many characters as possible. The regular expression .+ matches one or more occurrence of one character.For example, the regular expression bo+. matches bob, book, and boot. In this example, we combine the period (.) with the plus sign (+) to make one syntax. The period (.) appears immediately after the plus sign (+) expression. The plus sign (+) matches one or more occurrences of the letter 'o'. The period (.) acts as a wild card for the last character of each word, which, in this example are 'b', 'k', and 't'.
@	Minimal—zero or more matches zero or more occurrences of a character that precede the expression, matching as few characters as possible. The regular expression .@ means match zero or more occurrences of one character. For example, the regular expression a.@x matches 'abx' within '
#	Minimal—one or more matches one or more occurrences of a character that precede the expression, matching as few characters as possible. For example, the regular expression si.#er matches 'sicker' or 'silkier'. In this example, we combine the period (.) with the sharp sign (#) to make one syntax. The period (.) appears immediately before the sharp sign (#) expression. The sharp sign (#) matches one or more occurrences of any character between 'si' and '
[ ]	Set of characters matches any one of the characters within the brackets ([ ]). You can specify ranges of characters by using a hyphen (-), as in [a-z]. Examples: • The regular expression c[aou]t matches cat, cot, and cut, but not • The regular expression [0-9] means match any digit. You can specify multiple ranges of letters as well. • The regular expression [A-Za-z] means match all upper and lower case letters.
^	Beginning of line anchors the match to the beginning of a line. For example, the regular expression ^When in matches the any string that begins with "When in" and that also appears at the beginning of a line, such as "When in the course of human events" or "When in town, call me". Whereas, this regular expression does not match "What and when in the course of human events" if it appears at the beginning of a line.

Syntax	Expression Description
$	End of line anchors the match to the end of a line. For example, the regular expression professional$ matches the end of the string "He is a professional" but not the string "They are a group of professionals".
^^	Beginning of file anchors the match to the beginning of a file. Works only when searching for text in source code or in text files. For example, to match the first HTML tag at the beginning of a file, use the following regular expression: ^^
$$	End of file anchors the match to the end of a file. Works only when searching for text in source code or in text files. For example, to match the last HTML tag at the end of a file (with no spaces following the tag), use the following regular expression: $$
|	Or indicates a choice between two items, thereby matching the expression before or after the OR symbol (|). For example, the regular expression (him|her) matches the following occurrences it belongs to him or it belongs to her but it does not match the line it belongs to them.
\	Escape special character matches the character following the back slash (\ ). This allows you to find characters that are used in the regular expression syntax, such as a left curly brace ({) or a caret (^) or some other special character. For example, you can use \$ to match the dollar sign character ($) rather than implementing the regular expression to 'anchor to end of a line'. Similarly, you can use the expression \. to match the period (.) character rather than match any single character, which is what the period (.) regular expression does.
{}	Tagged expression tags the text matched by the enclosed expression. You can match another occurrence of the tagged text in a Find expression or insert the tagged text in a Replace expression using \N. For example, suppose you are looking to find two duplicate, consecutive words. To search, use the following expression: {.#} \1 With the assumption that the consecutive words are separated by a single space, you'll want to add a space between the right curly brace (}) and the back slash (\ ). In this example, we combine the sharp sign (#) and the period (.) with the curly braces ({}) to make one syntax. In this expression, .# represents any consecutive characters. Since this portion of the expression is surrounded by curly braces ({}), the consecutive characters will be tagged and can be referred to as \1. This expression will find any consecutive characters followed by a space, followed by those exact same consecutive characters.

Syntax	Expression Description
\N	Nth tagged expression in a Find expression, \N matches the text matched by the Nth tagged expression, where N is a number from 1 to 9. In a Replace expression, \N inserts the text matched by the Nth tagged expression where N is a number from 1 to 9. \0 inserts the text matched by the entire Find expression. For example, suppose you want to find two duplicate, consecutive words and replace them with a single word. To search, use the following expression: {.#} \l With the assumption that the consecutive words are separated by a single space, you'll want to add a space between the right curly brace (}) and the back slash (\ ). In this example, we combined the sharp sign (#) and the period (.) with the curly braces ({}) to make one syntax. To replace, use the following expression: \l \1 represents what was found in the first pair of curly braces in the find string. By using \1 in the replace action, you essentially replace the duplicate, consecutive words with a single copy of the word.
( )	Group expression marks the beginning and end of a sub expression. A sub expression is a regular expression that you enclose in parenthesis ( ), such as the expression that follows: (ha)+ In this example, we combine the plus sign (+) with the parenthesis ( ) group expression to make one syntax. The sub expression is (ha) because it is encapsulated within the parenthesis ( ). When you add the plus sign (+), the expression enables you to find repeating pairs of letters. The plus sign (+) represents one or more occurrences of 'ha'. This expression matches the following occurrences 'haha' and '
~x	Prevent match prevents a match when x appears at this point in the expression. For example, the regular expression real~(ity) matches the real in realty and really, but prevents the match to real in reality.
\n	Line break matches a new line in Code view, or a <br inDesignview. The syntax (\n), is a shorthand approach to enable you to match all line breaks.

Syntax	Expression Description
\t	Tab matches a single tab character. For example, if you want to find all single tabbed characters at the beginning of a line, the regular expression would look like the following: ^\t+ In this example, we combine the caret (^) and the plus sign (+) with the tab (\t) to make one syntax. The caret (^) that precedes the single tab character expression, anchors the match to all tabbed characters at the beginning of the line. The plus sign (+) represents the matching of one or more tab characters.
[^]	Any one character not in the set matches any character that is not in the set of characters that follows the caret (^). For example, to match any character except those in the range, use the caret (^) as the first character after the opening bracket. The expression [^269A-Z] will match any characters except 2, 6, 9, and any upper case alphabetical characters.
n	Repeat expression matches n occurrences of the expression that precedes the caret (^). For example, with n equaling 4, the expression [0-9]^4 matches any 4-digit sequence. In this example, we combine the set of characters ([ ]) syntax with the repeat (^n) syntax to demonstrate a more realistic use of regular expressions.
:a	Alphanumeric character matches the expression [a-zA-Z0-9]. You can use the following expression: [a-zA-Z0-9] to match one occurrence of a letter (upper case or lower case) or number. Also known as alphanumeric occurrences. You can use the shorthand expression :a for all instances of [a-zA-Z0-9].
:b	White space matches any white spaces in code or text. For example, to match a single white space character at the beginning of a line, use the following regular expression:^:b
:c	Alphabetic character matches the expression [a-zA-Z]When you use this expression, it enables you to match all upper or lower case letters. You can use the shorthand expression :c for all instances of [a-zA-Z].

Syntax	Expression Description
:d	Decimal digit matches the expression[0-9]This expression enables you to match any digit. For example, suppose you want to find a social security number in a text file. The format for U.S. social security numbers is 999-99-9999. :d^3-:d^2-:d^4 or, by using [0-9], the same resulting expression:[0-9]^3-[0-9]^2-[0-9]^4] You can use the shorthand expression :d for all instances of [0-9].
:h	Hexadecimal digit matches the expression [0-9a-fA-F]+ Use a this expression when you want to match a hexadecimal combination of any upper or lower case letters between 'A' and 'F', and any numbers. For example, suppose the pages in your website have multiple different background colors and you want to change the color of those pages to black, such as 000000. However, you do not know what the hexadecimal numbers are for the existing colors. Use the following regular expression to find all existing hexadecimal numbers: \#:h You could use [0-9a-fA-F] to search, but in this example we combine the back slash (\) and the sharp sign (#) with the hexadecimal digit (:h) syntax. \# matches a non-expression sharp sign (#) and :h matches any sequence of hexadecimal characters. To replace the existing hexadecimal numbers, type the hexadecimal number of the background color that you want: 000000
:i	Identifier matches the expression [a-zA-Z_$][a-zA-Z0-9_$]* When working with code, if you want to match all program identifiers, you can use the shorthand expression :i to replace having to type the lengthy expression above.
:n	Rational number matches the expression ([0-9]+\.[0-9]*)|([0-9]*\.[0-9]+)|([0-9]+) If you want to match all whole numbers that contain a decimal point, you can use the shorthand expression :n to replace having to type the lengthy expression above.

Syntax	Expression Description
:q	Quoted string matches the expression ("[~"]*")|('[~']*') If you want to match all quotes surrounded by quotation marks, you can use the shorthand expression :q to replace having to type the lengthy expression above.
:w	Alphabetic string matches the expression [a-zA-Z]+ This syntax is a shorthand approach to enable you to match one or more alphabetical characters, either lower case or upper case.
:z	Decimal integer matches the expression [0-9]+ This syntax is a shorthand approach to enable you match any number from zero or more.

Task Builder File Menu

The File menu comprises a variety of typical commands, such as **New**, **Open**, **Save**, **Print**, **Send**, and **Close**. It also contains an **Options** command which allows you to view or edit various Task Builder preferences, including formatting options, default fonts, color schemes and debugging alternatives. For convenience, the File menu lists the most recently opened tasks so that you don't have to search your computer for a task you previously opened or frequently work on.

The File menu can be accessed by clicking the **File**tab located in the upper-left corner of the ribbon.

File menu items

The following table provides a description for each command found when clicking **Application**along with their associated controls and keyboard hot-keys (if applicable).

Command	Description	Hot-Key
Help	Opens the embedded help files.	---
New	Creates a new task. Selecting this option adds a new tab in the Steps pane. **NOTE:** Using this option creates an unmanaged task.	CTRL + N
Open...	Opens an existing task. A standard Windows Explorer dialog appears allowing you to navigate to the task (.AML) file to open.	CTRL + O
Save	Saves the current task. If the task being saved is a managed task, it will be saved to its present location. If saving an unmanaged task (that is, created using the **New** option), a standard Windows Explorer dialog appears allowing you to select the folder in which to save the task (.AML) file.	CTRL + S
Save Copy As	Saves a copy of the task file or saves the task file in another format. A standard Windows Explorer dialog appears allowing you to navigate to the location in which to save the task (.AML) file.	SHIFT + CTRL + S
Save All	Save all open tasks.	---
Print	Prints the steps of the current task as they appear in the Steps pane.	---

Command	Description	Hot-Key
Send	Emails the current task to the specified recipient. The available send options are: • **Mail Recipient** - Sends the displayed task in the body of an email. • **Mail Recipient (As Attachment) -** Sends the displayed task as an email attachment. • **Mail All to Recipient (As Attachment) -**Sends all open tasks as email attachments.	---
Tools		
Close	Closes the current task file. If changes were made, a dialog will appear prompting whether to save the changes. Click **Yes** to proceed.	---
Close All	Closes all currently opened tasks. If changes were made to one or more tasks, a dialog will appear prompting whether to save the changes. Click **Yes**to proceed.	---
Options	Allows access to available Task Builder Options. The table below lists available options.	---
Exit	Closes the Task Builder.	---

Available Task Builder Options

Below lists the various categories of Task Builder options in alphabetical order, with links to the topics covering each:

Option	Description
General Options	Contains options that determine certain behavioral characteristics of Task Builder. Also determines the default managed task location.
Formatting Options	Contains options that deal with how steps should be formatted in the Steps pane.
Fonts Options	Contains options to modify the font name, size and style to be used for the Visual view and the AML view.
Color Options	Contains options that determine the color to be used for the Task Builder interface or allows adjustments to be made to the current color scheme.

Option	Description
Layout Options	Resets the Task Builder panels back to the default settings.
Debugger Options	Contains options that affect Task Builder's behavior while running and debugging tasks.
Toolbar Options	Contains options that determine the look and feel of Automate Desktop's debugger toolbar.

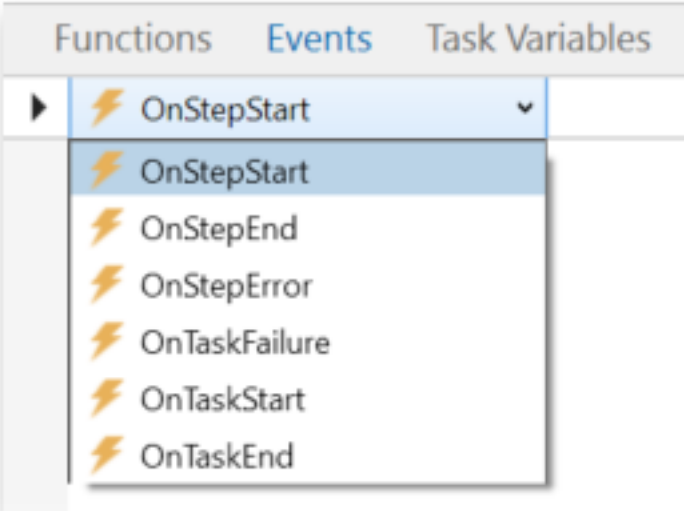
Task Events

Task events along with task functions are core features in programming that make complex, high level automation routines more comprehensible. They enable the flow of a program to be determined by specific events that take place, which in turn, triggers execution of a callback function.

The Task Builder is capable of raising task events as it performs the steps necessary to complete a task. This capability allows specific event-driven information to be returned when a task starts, when it completes (either successfully or unsuccessfully) or during various other stages in between (for example, when a task step starts, ends or generates an error). Tasks become more robust when task events are implemented. This is because events make a task more intelligent with their ability to monitor execution status and provide notification when a status has changed.

Task events are managed through a drop-down menu that is accessible from the Steps panel of Task Builder.

NOTE: Task Events are additional features aimed for advanced users. You can build tasks without the use of Task Events and may choose to use these features at your own pace.



To set a task event

1. From the Task Builder's Steps panel, select **Events**.
2. Click the drop-down combo box to display a list of pre-defined task events (see the table below for more details).
3. Select the desired task event.

Parameters

The following table describes available task event parameters:

Property	Type	Description
Name	Text	The name of the parameter.
Return type	Text	The return value type. Task event value types are always in the form of a variable.
Is Optional	TRUE/ FALSE	Specifies whether the parameter is optional (TRUE) or required (FALSE). This option is always marked FALSE for task events.
Default value	Text	The task event's default value.
Description	Text	A description of the parameter.

Available Events

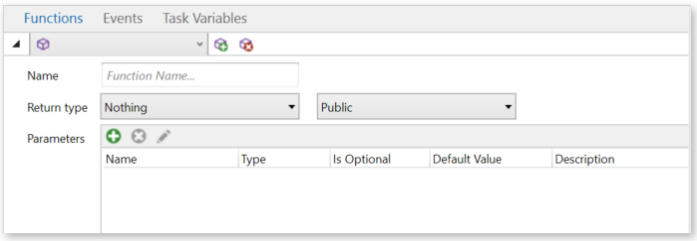
The Task Builder provides six task events in which you can subscribe (also known as pre-defined task functions). The following table lists the available task events along with their description. For additional information regarding a specific task event, click the event's associated link.

Event	Description
OnStepStart	This event is fired each time a step executes.
OnStepEnd	This event occurs each time a step is completed.
OnStepError	This event occurs each time a task step generates an error.
OnTaskFailure	This event is fired each time a task step causes an error. Depending on how the step is configured, the task may either continue after the error occurs or may be aborted. In the latter case, the **OnTaskEnd**event is fired immediately after.
OnTaskStart	This event is fired when a task is started. This is normally the first event fired when task execution starts.
OnTaskEnd	This event is fired when a task ends.

Task Functions

In programming, functions allow the structuring of programs in segments of code to enable performance of individual tasks. A function has input and output, and contains instructions used to create the output from its input (that is, performs a calculation on the input and returns an output). The same holds true for task functions in the Task Builder. Each task function performs an operation and optionally returns a value. The output value can be private, or it can be made public and stored in a variable to be called upon by as many steps as required by the task.

Task functions are created and managed through a drop-down interface accessible from the Steps Panel of Task Builder.



> **NOTE:** Task Functions are supplemental features aimed for advanced users. You can build tasks without the use of Task Functions and may choose to use these features at your own pace.

Scope and Accessibility

The power of task functions comes from their ability to provide variable modularity and protection and their capability to arrange a collection of task steps into a logical structure. This is accomplished through two distinct yet complimentary standards; scope and accessibility. Scope and accessibility are primary building blocks that allows you to construct a solid foundation and enable a rich object-oriented approach to tasks. They provide distinct capabilities and serve different but complimentary roles necessary to distinguish the benefits of task functions.

Scope

A scope in any programming is a region of the program where a defined variable can have its existence and beyond that variable can not be accessed. In Automate Desktop, scope limits a task function's visibility within a task. Without proper scoping, some of the primary advantages of function-oriented design would not be possible, including information-protection, modularity, maintainability and recursion. Scoping helps take large, unruly tasks and enforce logical restrictions to their structure to provide greater readability and maintainability. Scoping also helps avoid unintentional and confusing

data changes leading to easier debugging as well as construction of cleaner and more reliable tasks.

Accessibility

Accessibility provides the fundamentals of information-protection, encapsulation and interfacing, all of which are essential for an object-oriented approach to a language. It makes tasks more portable, manageable and documentable by providing outside access only to those parts of the task that are meant to be used, while providing the user full flexibility of functions. Task functions exist at the root of a task structure, thus, their scope is to the entire task. However, their accessibility, which defines whether or not the function is accessible and visible to an external task, can be defined in the following manners:

- **Public**- Visible and accessible to external tasks.
- **Private**- Not visible or accessible to external tasks. Access is limited to the containing type.

The ability to set task functions as **public**or **private** give developers greater control over how a task is used by another task.

Sub-Tasks

Sub-tasks are task files that are executed within another task by using the Task - Start sub-task activity. In this situation, the parent task's (that is, the task executing the Start sub-task step) basic functions, extended functions, public task functions, public task variables, and any local variables (not marked as private), created up to point where the Start sub-task step is encountered, are accessible to the sub-task. All other variables and functions are not accessible to the sub-task. Conversely, because the Start sub-task action is a synchronous operation, the sub-task's public functions and public task variables are not accessible from the parent task. This is fully backward compatible with previous versions of Automate Desktop, since in the past there was only one "function" (what is now called "main"), no task variables, and all (local) variables and extended functions were considered public.

When you define a task function, you can optionally define one or more named, typed values that the function receives as input (known as argument parameters). You can declare arguments as optional and set a default value for any argument - so if the argument is not present, the default value will be used. You can also define a type of value that the function will pass back to the task as output upon completion (known as return type).

Function argument parameters and return values are extremely flexible in Automate Desktop. You can define anything from a simple utility function with a single unnamed parameter to a complex function with expressive parameter names and different

parameter options. You can provide default values to simplify function calls and can be passed as in-out parameters, which modify a passed variable once the function has completed its execution.

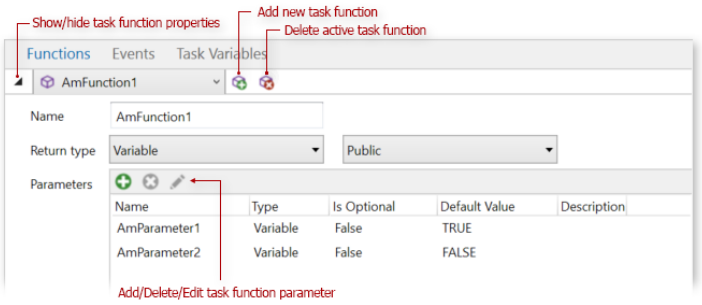
Creating and Defining Task Functions

When you define a task function, you can optionally define one or more named, typed values that the function receives as input (known as argument parameters). You can declare arguments as optional and set a default value for any argument - so if the argument is not present, the default value will be used. You can also define a type of value that the function will pass back to the task as output upon completion (known as return type).

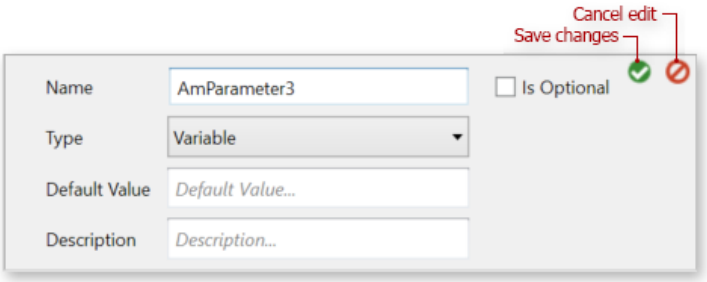
Function argument parameters and return values are extremely flexible in Automate Desktop. You can define anything from a simple utility function with a single unnamed parameter to a complex function with expressive parameter names and different parameter options. You can provide default values to simplify function calls and can be passed as in-out parameters, which modify a passed variable once the function has completed its execution.

To create and define a new task function

1. On the Task Builder's Steps panel, select Functions.
2. Click the **Add new function** button. This expands the UI panel to display available function properties.



3. Enter a function name, select a return type and specify whether the function is public or private (see the Function Properties table below for more details).
4. To add argument parameters, click the **Add new parameter** button. A dialog appears that allows you to enter function parameters.



5. Enter the required information and click the **Save Changes** button upon completion (see the Argument Parameters table below for more details). Perform steps 3-4 to add additional parameters. To edit or remove an existing parameter, select it from the list and click the **Edit**or **Remove** button.

To modify an existing task function

1. On the Task Builder's Steps panel, click the drop-down button to expand the list of existing task functions/events.
2. Select the task function you wish to modify, then click the (**View Function Properties**) button.
3. Perform the appropriate modifications.

To delete an existing task function

1. On the Task Builder's Steps panel, click the drop-down button that displays existing task functions/events.
2. Select the function you wish to delete.
3. Click the (**Remove Task Function**) button. This will permanently delete the task function.

Function Parameters

The following table describes the parameters available during task function creation/modification.

Property	Type	Description
Name	Text	The identifier by which the function can be called. This parameter defaults to the name *NewFunction* but can be modified to a name that better identifies the function.

Property	Type	Description
Return type	Text (options)	The return value type. The available options are: • **Nothing**- No value (nothing) will be returned. • **Variable**- The return value will be in the form of a variable. • **Array**- The return value will be in the form of an array. • **Dataset**- The return value will be in the form of a dataset.
Function is private	Yes/No	If selected, the function becomes private.

Argument Parameters

The following table describes the parameters available during task function creation/modification.

Property	Type	Description
Name	Text	The identifier by which the function can be called. This parameter defaults to the name *NewFunction* but can be modified to a name that better identifies the function.
Type	Text (options)	The return value type. The available options are: • **Nothing**- There will be no return value. • **Variable**- The return value will be in the form of a variable. • **Array**- The return value will be in the form of an array. • **Dataset**- The return value will be in the form of a dataset.
Is Optional	TRUE/FALSE	Specifies whether the parameter is optional (TRUE) or required (FALSE). Any call must provide arguments for all required parameters, but can omit arguments for optional parameters. Each optional parameter has a default value as part of its definition. If no argument is sent for that parameter, the default value is used. When you define a complicated function, you will often want to set this to optional (TRUE) for flexibility.

Property	Type	Description
Default value	Text	The function's default value (if any).
Description	Text	An optional description to enter about the parameter.

Calling Task Functions

A function doesn't do anything until it is called. Every function has a function name which may describe the procedure that the function performs. To use a function, you “call” that function with its name and pass it input values (known as arguments) that match the types of the function’s parameters. If you are calling a function with no parameters, an empty pair of parentheses is required.

The Task - Call function activity calls a function defined in the task. If the function returns a result, you can specify the name of the variable in which to place the value. This activity is mainly used to pass control to a subroutine; after the subroutine is executed, control returns to the next instruction in main task.

In addition, the Variable - Return activity can be used to exit the current function and return task execution to the calling function. A return value can also be specified to the caller. This activity immediately ends execution of the current function and returns its argument as the value of the function call.

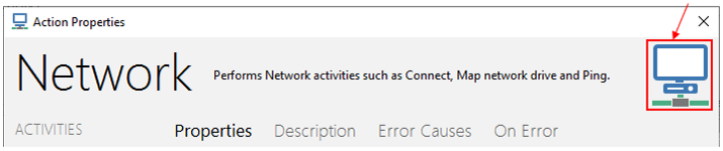
Actions

The work items performed by a task are called actions or activities. They are the basic building blocks that enable development of intuitive tasks without the need to write code. Actions are organized in a hierarchical format in the Task Builder, each action containing individual activities (or sub-actions) which are subroutines directly related to the main action. You simply drag-and-drop actions / activities from the Task Builder Actions Panel onto the Task Builder Steps Panel to build a series of steps, which collectively make up the task.

> **NOTE:** The Help for the Actions is stored in **..\Program Files\Globalscape\AutoMate\Help**. Click **Default.htm** to open the help in your default browser.

> **NOTE:** Other than for testing event rules, the Advanced Workflows actions that require user input (such as the Dialog Message action) should not be used in EFT actions. If the event rule is running while the EFT interface is closed or unattended, you won't know the action is waiting for a response, and therefore the event rule will timeout.

Actions and activities perform operations such as starting applications, sending keystrokes, clicking controls, uploading files, and much more. They can be further expanded by the use of variables, constants, and expressions. A task may comprise a single action or it may involve multiple actions and more complex elements such as variables, expressions, conditional logic, looping, and more.

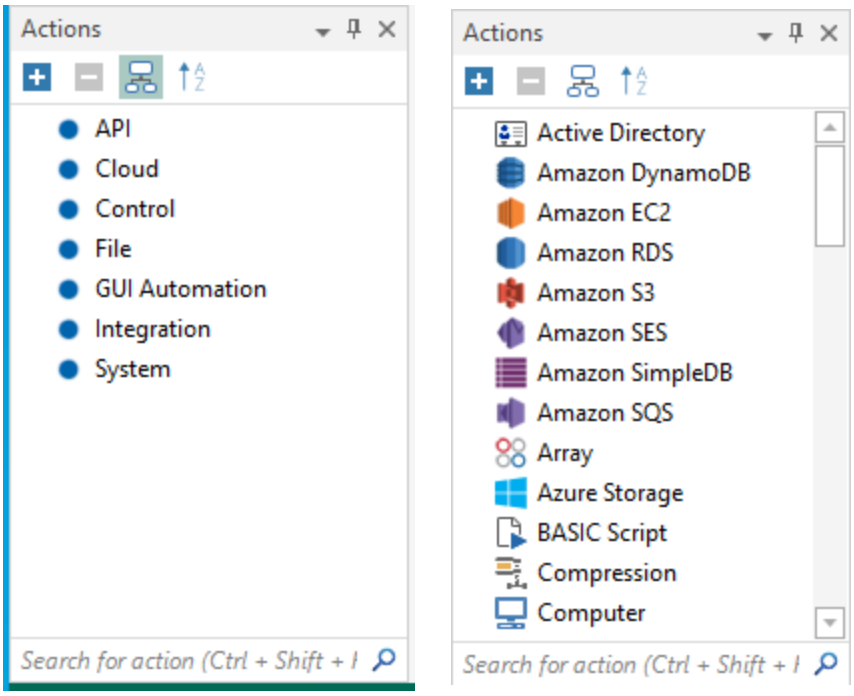
> **NOTE:** Refer to the Task Builder help content for details of the Advanced Workflow actions. You can also click the action's icon to go directly to the help for that action.
>
> 
>

Available Actions

The following table lists all of the actions available along with a brief description. To view more information about a specific action or to access the available activities (or sub-actions) for each action, open the action in the Task Builder and open the Help file.

In the Task Builder, the Actions are organized in the Actions panel by categories. You can expand the categories by clicking the organize icon to view the actions in

alphabetical order. Or you can search for an action in the Search box at the bottom of the panel.



Name	Description
Active Directory	Automates a variety of common Active Directory tasks is available, such user account creation / provisioning and deprovisioning. Most Active Directory related jobs are often repetitive and time-consuming, so automating them does a world of good to network administrators and their enterprise, in terms of time saved and standards achieved.
Amazon DynamoDB	Allows developers to automate a variety of DynamoDB operations without the need to write code. Since DynamoDB is a service based on throughput, developers can also create tasks to monitor usage and storage capacity.
Amazon EC2 (Elastic Compute Cloud)	Allows developers to automate the management of EC2 instances, improving efficiency while maintaining a high level of performance. Using these activities, one can optimize the use of compute resources in a variety of circumstances.
Amazon RDS (Relational Database Service)	Provides cost-efficient and re-sizable capacity while automating time-consuming database administration tasks, freeing you up to focus on your applications and business.
Amazon S3 (Simple Storage Service)	Provides developers the tools to automate to automate common S3-related operations such as the creation and management of buckets and the objects that reside in them.
Amazon SES (Simple Email Service)	Enables automation of many common aspects of email management, such as creation, verification and retrieval of identities for a specific AWS account as well as composing and sending email messages based on input data.

Name	Description
Amazon SimpleDB (Simple Database)	Contains a variety of activities that enables automation of common to complex SimpleDB operations, eliminating the administrative burden of performing manual operations such as data modeling, index maintenance, and performance tuning.
Amazon SQS (Simple Queue Service)	Automates the creation of queues and movement of data between distributed components of relevant applications that perform different tasks without losing messages or requiring each component to be always available.
Array	Enables creation of arrays to be used during task execution, allowing a group of objects with the same attributes to be addressed individually. It can also set an array to a specific value or modify the current size of an array.
AS2 (Applicability Statement 2)	Allows users to automate EDI/AS2 related operations, such as creating and sending messages, decoding messages and verifying receipts.
Automate	Comprises individual activities that enables automation of common processes that are specific to the Automate Desktop program, such as writing to the Automate Desktop log or shutting down Automate Desktop.
Automate Schedule	The Automate Schedule action enables additional automation capabilities with Automate Schedule through Automate Desktop. Automate Schedule's integration with Automate Desktop will allow users to create server objects (in Automate Schedule) that represent an Automate Desktop / Automate Enterprise installation and have the ability to build jobs that execute a task / workflow on selected Automate and Automate Enterprise servers. Automate Scheduleis aware of defined Automate Enterpriseservers, and can run tasks or workflows on those servers, wait until the task is complete before moving on to the next command in the Automate Schedule job, capture the return code of the task or workflow and capture the command line output and add it to the job log.
Azure Storage	Enables cloud storage automation with a comprehensive set of Windows Azure Storage activities, including blob, entity, table, queue and message- related activities.
BASIC Script	Often used to create sophisticated scripts without the need to write VBScripts, Shell Scripts, batch files or any type of code. In addition, it can also incorporate existing VBScripts, Powershell and other scripts into manageable task flows and add new functionality to old applications with the use of over 500 available actions and activities.
Clipboard	Contains various activities that can automate all Windows clipboard operations. Along with the basic Cut, Copy, Paste, and Clear clipboard activities, this action comprises the Get contents activity, which retrieves the current contents of the clipboard as text and places it in a variable, and a Set activity, which allows you to set the clipboard to the text specified.
Compression	Automates the ability to compress and / or decompress data in a specific directory. It supports all major compression types, including ZIP, JAR, GZIP, TAR and 7ZIP (among others). Other features include the ability to password protect encrypted data and change the level at which files are to be compressed.
Computer	Allows the ability to automate various Windows start menu power button functions such as Lock, Restart, Shut down, Log off, Suspend, and Hibernate.

Name	Description
Cryptography	Automate Desktop's encryption and decryption of files. Can also create or delete key containers, generating both public and private key files from existing key containers and digitally signing files using newly generated private keys. Supports PGP (Pretty Good Privacy), one of the most widely used cryptography systems.
Database	Enables creation of sophisticated database-driven applications without the need to write code. Supports SQL Server, Oracle, Access, Sybase, DB2 and other ODBC-based database. This powerful tool can automate report generation and distribution, run DTS or similar database maintenance processes automatically and expand tasks to do even more using Automate Desktop's library of actions and activities.
Dataset	Automates the creation or cloning of a dataset, as well as managing the rows and columns within it.
DDE (Dynamic Data Exchange)	Enables automation of operations that a DDE client usually performs, such as the ability to send requests and commands to DDE Server applications.
Dialog	Contains various dialog activities, each displaying its own unique dialog window during runtime. The type of dialog displayed is dependent upon the desired user interaction. Additionally, a Custom Dialog activity can be used to create your own dialogs in situations where a normal Windows message box may not be sufficient enough.
DLL (Dynamic-link Library)	Executes the specified method in a managed or unmanaged dynamic-link library (DLL) and stores the return value of the method in an Automate Desktopvariable.
Dynamics CRM	Automates a variety of common CRM operations in order to ensure consistency in how businesses interact with their customers. It can be used for creating, updating or deleting contacts, retrieving audit records, tracking specific information, and uploading and downloading attachments.
Email	Combined with the Exchange action, Automate Desktop presents an effective email attendant that allows you to automate common to complex email operations and simultaneously manage several email accounts from as many mail servers as required.
Environment Variables	Automates the creation, manipulation and management of environment variables in a Microsoft Windows-based operating system without the use of scripts or the command line. Activities include the ability to get, set, list and delete environment variables as well as append data to an existing environment variable.
Event Log	Allows custom events to be logged in a purely automated fashion. Developers can control the type of event to log by specifying a level value such as warning or error. Furthermore, this action can be used along with the Event Log trigger as a way to launch other tasks upon arrival of a specific event.
Excel	When you work with Microsoft Excel, you usually select one or more cells and then perform an action, such as formatting the cells, entering values in them or retrieving current values. The Excel action encompasses a variety of activities that are capable of automating such operations, thus, saving time and eliminating errors. In addition, this action is capable of running existing Excel macros as part of a fully automated sequence.

Name	Description
Exchange	Comprises a variety of activities that can be used to automate common operations on Microsoft Exchange objects, such as the ability to create calendars or appointments, delete contacts, modify tasks and retrieve email. This action supports Exchange 2003 which uses the WebDav protocol as well as Exchange 2007 and 2010, which uses the EWS (Exchange Web Service) protocol.
File System	Encompasses a comprehensive collection of activities for automating all file and folder-related operations. Activities include the ability to copy, delete or rename files and folders, read from a file and write to a file. Other activities include the ability to retrieve information about files, such as metadata and checksum values as well as the ability to split or concatenate files and synchronize folders (among others).
FTP (File Transfer Protocol)	Used to automate any FTP operation including downloads, uploads, renames, folder creations, deletions and more. Automate Desktop's internal FTP engine is compatible with all FTP connection methods, particularly security-based connections. This includes both explicit and implicit FTPS (FTP Secure or FTP SSL) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.
HTTP (Hypertext Transfer Protocol)	Contains activities that are ideal for automating common HTTP operations, such as GET, PUT, POST, DELETE and more. HTTP requests are sent directly instead of automating a browser to perform such operations. This action also supports Hypertext Transfer Protocol Secure (HTTPS) protocols, which is a combination of HTTP with the SSL/TLS protocol to provide encrypted communication and secure identification of a network web server.
If	In programming, the **If**statement is used to run code based on conditions. This allows programs the ability to perform different operations in response to different conditions. Automate Desktop's If activities encompass the same capabilities but with a more user-friendly approach. They enable complex decision making based on variable data in the context of a task.
Image	Developers and designers must deal with editing and converting many images by hand, which can be time consuming. Automate Desktop's Image action consists of activities that can greatly reduce the time it takes to perform such a process. For example, you can create a single task that reduces the size of an image, applies a filter for a particular effect and converts the image file to the desired format. In addition, you can integrate loop related activities to run this task on hundreds or thousands of images.
Input	With the Input action, automation of GUI-related tasks can be performed by simulating mouse movements, mouse clicks, and keyboard key presses, enabling you to control your PC with simple commands such as start, click and write. You select the proper activities to replicate the actions (that is, Move mouse, Click Mouse, Send keystrokes) that you would normally perform manually. Once you have entered a few steps, you can save them or easily test playback at the click of a button. This makes you more productive and lets you do something more meaningful or enjoyable with your time. Use this action combines with the Interactivity action to automate simple to complex GUI related operations.

Name	Description
Interactivity	Automate Desktopincludes numerous interactive-related activities that can impersonate object selection or any form of desktop interaction that one would normally perform manually. The Move mouse to object activity simulates moving the cursor to a specific object or control in a window. The Press activity simulates moving the cursor to an object and clicking that object all within one step. Such activities communicate with the target control natively, therefore, the window where the control resides is not required to be in the foreground for the event to occur. Other activities such as Get text and Set text allows you to easily extract text from and input text to a specific window on your desktop. Use these activities combines with the Input activities to automate simple to complex GUI-related operations.
JSON	Contains activities that allow you to decode and encode JSON (JavaScript Object Notation) objects
Label	Labels are used to label a step in a task with a specific name. A label is used with a Goto activity and/or the On Error Goto option (found in the On Error properties) to allow redirection of task execution to the label specified.
Loop	In computer programming, a loop is a fundamental yet powerful technique that is commonly used in writing programs. A loop is a sequence or "block" of instructions that is continually repeated a specified number of times or until a certain condition is reached. It allows a very simple operation to produce a significantly greater result simply by repetition. Similar to the concept of loops in programming, the Loop action in Automate Desktop allows repeated execution of a group of steps. Activities include the ability to loop through datasets, files, processes, lists, and more for dynamic automation.
MSMQ (Microsoft Message Queuing)	MSMQ (Microsoft Message Queuing) technology enables applications to communicate with each other in an effective and dependable manner, even in unreliable distributed environments where intermediate servers or systems may not always be available. This is made possible due to the fact that messages are not exchanged directly between applications but rather through a message queue, which is a temporary storage location from which messages can be sent and received reliably. Applications that run at different times can essentially send messages to queues and receive messages from queues at their convenience. Automate Desktop's MSMQ action provides a reliable and secure way to automate message delivery and retrieval by way of MSMQ. It contains individual activities that lets you to create, send, retrieve, clear, delete, or wait for MSMQ messages on a local or remote machine.
Multimedia	Automates the action of controlling the optical drive, play specific audio and / or adjust the system volume. In an automated environment, these activities can be used as notification tools. For example, a Play audio or CD control activity can be used in a task as a way to alert the user. They can also be used as an alarm clock or server audio notification.
Network	Contains activities used to automate various network related operations, such as establishing a network connection, mapping, or unmapping a network drive or sending a "ping" request to a computer.

Name	Description
OCR (Optical Character Recognition)	Provides new opportunities and techniques with regards to combining OCR capabilities in an automated environment. It enables you to convert typewritten, handwritten or printed text as well as text contained in images to an Automate Desktop variable or dataset, making it possible to search for a word or phrase, store text more compactly, and apply techniques such as text mining or text to speech.
OpenDocument Spreadsheet (ODS)	The OpenDocument Spreadsheet action is similar to the Excel action. Unlike the Excel action, however, the OpenDocument Spreadsheet action enables creation and management of spreadsheets without requiring Microsoft Excel to be installed on the system. This action not only supports spreadsheet generation and other basic file formatting features, but also supports a number of advanced features such as importing as well as exporting spreadsheet data, reading, writing, and modifying XLSX, XLS, ODS, CSV, or HTML files. This makes it much more convenient for developers to manipulate spreadsheet contents, format cells, and protect files.
PDF (Portable Document Format)	Automates an assortment of common PDF operations. Activities include the ability to concatenate or merge two or more PDF files, append new pages to an existing PDF file, extract pages, insert pages at a particular location in an existing PDF file or split one PDF into two or more PDF files (to name a few). For added Security, this action provides the ability to encrypt and decrypt PDF files with either 40-bit,128-bit, or 256-bit encryption and also specify user passwords for further protection.
PowerShell	PowerShell is a command line shell and scripting language for Microsoft Windows that is built on the .NET framework. PowerShell's task automation framework allows administrators to perform administrative tasks on both local and remote Windows systems. Automate Desktop enables management and control for PowerShell processing. With the use of the PowerShell action, you can embed existing PowerShell scripts to a task or point to an external .PS1 file to allow for seamless integration with other actions. To run unattended or scheduled PowerShell operations, simply add a schedule trigger.
Printer	Can optimize printing resources and print documents when they are required, not necessarily when they are generated. This action includes activities that can automate print jobs across various print queues, change the default printer or remove a specific printer on the fly. It also contains an activity that can retrieve status sand other properties about any printer across the network so you can better manage which printers and at what time print jobs should take place.
Processes	Enables automation of most process management operations. This action comprises activities that can automate the act of starting, stopping or controlling a process as well as query a process for specific types of information, such as names of loaded modules, number of consumed handles and sets of threads, start time and much more. You can also adjust the priorities of running programs so that badly behaved processes won't negatively impact the responsiveness of your computer. The available activities for this action supports management of local or remote processes.

Name	Description
Registry	Encompasses a variety of activities capable of automating many common registry configuration and management operations, such as the ability to create, manipulate, rename, and delete registry keys, sub-keys or value data. This action also allows registry values to be read and stored, which is ideal in situations when you may need to retrieve configuration data, for instance, to keep track of the software you install on the computer or save data collected from an external application so that it can be retrieved and used the next time the task is run.
Run	Runs the program, application or document specified. If a document is specified, the application associated with the document will be used to open it. This action comprises some built in conveniences, such as the ability to wait for an application to finish loading (that is, be ready for input) or wait for it to complete its operation before continuing to the next step. Commonly used to start an application or open a document in preparation to send keystrokes, mouse clicks or other interactive steps.
Security	Enhances the security of an automation routine by generating a strong password and / or suspending task execution until the user properly authenticates himself / herself by either entering the correct password. Can also be used to suspend execution until a specific a specific user is logged on.
Select	A useful alternative to using an "If" statement in a task. Like any If activity, this action allows decisions to be made during task execution depending on the result of an expression. The difference is the speed and readability of the resulting task when one of several decisions can be reached. For example, for a simple expression such as 1=1 (true) or 1>2 (false), it would be best to use the If activity. For more complex decisions where there are several possible answers such as favorite color=red, blue, green or yellow, Select / Case activities would be a better choice. This is because Select / Case presents the task steps in a manner that is more readable, and at runtime, the evaluation of the expression occurs only once rather than needing repeated If activities with individual comparison.
Services	Provides various ways to automate the management of local or remote services. Using a variety of activities, you can easily automate operations such as starting, stopping, installing, or uninstalling services. You can also query for a list of services installed on the system along with their current state.
SharePoint	Comprised of over 40 activities that enables automation of simple to complex SharePoint operations. For instance, this action can automate the creation, management and implementation of SharePoint sites that are discoverable throughout the organization. By further streamlining and automating SharePoint processes, a company's resources can be allocated to other areas, which can lead to reduced costs and greater operational efficiency.
SNMP (Simple Network Management Protocol)	Used to automate common SNMP commands such as GET, GET BULK, GET NEXT, SEND TRAP, SET, and WALK, providing server administrators and IT personnel a means to monitor a complete network infrastructure through simple Automate Desktop tasks. Also enables integration of Automate Desktopwith products such as Microsoft MOM and others.

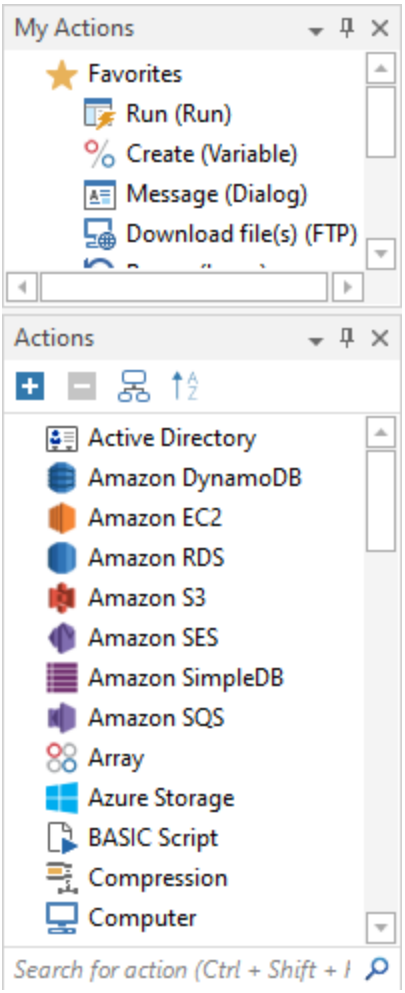
Name	Description
Speech	Enables interactions to be performed during runtime by way of the Windows speech synthesis engine. Common uses would be to create a blind-accessible system to read text data from the screen, create audible reminders, and notifications, and web / document reader applications.
Task	Allows task level operations to be automated during runtime. Activities include the ability to start a secondary task (also known as a child task or subtask) from a parent task or start another task as a separate thread. Other activities can disable / re-enable execution of other tasks. For instance, a Disable task activity could be placed at the beginning of Task1 to disable execution of Task2 for the time being to ensure it doesn't interfere with execution of Task1. An Enable task step could be placed at the end of Task1 to re-enable execution of Task2.
Terminal	Often used to completely simulate the procedures that a user typically performs during a terminal session. The Terminal action allows legacy systems to be automated in the background without the need for 3rd party software. With Automate Desktop, terminal servers can be used to run programs, save files, and employ network resources, altogether, working as a bridge to connect terminal, and / or legacy systems to Microsoft Windows networks and computers.
Text	Text manipulation is a way to administer and modify textual data, including text conversion, transformation, and extraction. Some common text operations involve stripping of characters or white space, converting words to upper or lower case, adding or replacing characters, and calculating character count for the selected text. Automate Desktop encompasses a variety of activities primarily designed to automate the management, modification, and enhancement of text. These time saving activities are the complete solution for any data and text editing procedures that are performed in large quantities or in a repetitive manner.
Timer	A timer can be used to examine the sequence of an event or process taking place. This is an ideal way for developers to gauge the total execution time of an individual task step or series of steps that perform time sensitive operations. A Start Timer activity creates a new session and begins the recording process and a Stop Timer activity marks its ending. The elapsed time is then output to an Automate Desktop variable. In addition, a Read Timer activity can be used to gauge the execution time between Start Timer and Stop Timer steps. Multiple timer operations can occur simultaneously within the same task as long as each operation is designated by a unique session.
Twitter	Performs automated status message updates on a valid Twitter account. This action can update a status message upon schedule or when a certain event occurs. For example, the Twitter action can be used to perform internal updates on network issues for IT staff or external Twitter communications on new products or other subjects for marketing purposes. This action can also be used to perform a variety of other Twitter operations, such as Get Status, Delete Status, Send Direct Message, Get Followers, and much more.
Type	Used to create an Automate Desktop object from the defined custom type or web service. This action can also be used to define a custom object type or object types defined in a Web Service or import Web Service or .Net assembly types.

Name	Description
Variable	The Variable action comprises various activities geared for the creation and management of variables and / or arrays. The developer can enter a value to initially populate the variable during creation or the value field can be left blank. Instead, variables can be set with a value using the Set Variable activity, which adds or changes the contents of an already existing variable. Certain available actions that support populating variables can also set or modify a variable's contents, such as the Input Dialog activity, which displays an input box allowing the user to enter a value which is saved to the variable specified.
VMWare Guest	Useful for automating many common operations on a VMware guest operating system, such as running a program or script, managing processes, creating, and managing files and directories, creating screen shots, administering environment variables, and much more. With these activities, you can run common tasks on a network where you have multiple virtual machines running on one or more physical machines. Automate Desktopsupports the full suite of virtualization software including ESX, ESXi, Workstation, and Player.
VMWare Host	Useful for automating many common performance and auditing operations on a VMware host operating system. For instance, you can create a task to automate the process of modifying a limitless number of hosts, freeing up time for more strategic activities. Automate Desktopcan automatically generate lists of running hosts as frequently as required as well as automatically register and unregister hosts based on any event defined. Other activities include the ability to start, resume, or suspend a VM, take snapshots, revert to a previous snapshot, and much more.
Wait	In programming, a wait state is a situation in which a program waits for the occurrence or completion of a specific event or condition before continuing. Because the result of a wait can largely impact task execution, many Automate Desktop activities have their own built-in wait capabilities. In addition to the built-in wait function, a number of individual 'Wait' activities are also available which can be used at any point inside a task without the need to write code. These activities provide additional intelligence to Automate Desktop's already powerful task flow capabilities by allowing execution to pause until a specific date / time, until the existence (or non-existence) of a file or window, wait for a process to start or end, or wait for a specific amount of time.
Web Browser	Can be used to automate basic to complex web-based operations. Using these activities, any combination of web-related actions that one normally performs manually, such as browsing, form filling, clicking and data extraction, can be simulated at runtime. Provides automation support for Chrome and the latest version of Firefox by no longer requiring a separate extension to be installed. **NOTE:** The Web Browser action is not backwards compatible with the Web Browser (Legacy) action.

Name	Description
Web Browser (Legacy)	Can be used to automate basic to complex web-based operations. Using these activities, any combination of web-related actions that one normally performs manually, such as browsing, form filling, clicking and data extraction, can be simulated at runtime.
Web Service	The benefits of Web Services to any business can be summed up in one word: efficiency. Automate Desktop helps leverage this functionality with its Web Service - Execute function activity. This action allows you to automate the ability to execute Web Service calls by way of WSDL (Web Service Definition Language) URI (Uniform Resource Identifier) path. With Automate Desktop, once you enter a WSDL URI path and select **Go**, it automatically evaluates that Web Service and fills in the information for you to select from a list.
Window	Interactive tasks are defined as tasks that simulate mouse movement, mouse clicks, keyboard activity, or any type of interaction with the desktop. Performing interactive actions normally requires the use of the Input and Interactivity actions. However, in order for interactions to be performed accurately on a specific window, that window must usually be "focused" or in front of all other open windows. The Window action is used ideally in such situations. It encompasses a variety of activities used to manipulate windows on the desktop such as moving, minimizing, maximizing, hiding, focusing, or closing a window. The Window action as well as all other interactivity related actions implement Automate Desktop’s Window Dissection Technology, which allows the specification of a window based on title as well as objects, controls, and / or text that are inside of it. Window Dissection ensures that all interactive tasks execute with accuracy at runtime.
WMI (Windows Management Instrumentation)	Can be useful for monitoring and controlling managed resources on a local or remote computer, thus, improving manageability of computers in a networked environment. For instance, a WQL Query task can initially determine any issues and direct itself to perform proper activities to correct the problem before proceeding to other steps.
XML (Extensible Markup Language)	Automate Desktop's XML action enables automation of many common XML related activities, such as transforming, merging, validating, and signing XML documents. They are also capable of reading, creating, editing, or deleting XML nodes as well as extracting XML fragments (that is, a collection of XML nodes) and saving them to a file or other means. The XML activities provide all of the features and functionality necessary for managing and manipulating XML.

Actions Panel

A task is something that performs a number of sequential steps that are necessary to reach a desired outcome. The Actions panel houses all of the available actions and associated activities that make up the steps to be performed during task execution. Actions and activities are assembled visually by dragging them from the Actions panel onto the Steps panel (or by simply double-clicking the desired action/activity) and entering their properties. When this is accomplished, the action becomes a task step. This panel also contains a My Actions view which puts your favorite, recently used and most used activities along with any saved snippets in a convenient location for easy access.



Actions view

The Actions view is comprised of over 400 built-in actions and activities, which range from starting an application, opening a web page, focusing on a window, uploading or downloading files, sending and receiving email, simulating mouse or keyboard activity

and much more. Actions and activities are arranged in a hierarchical format so that users can browse through them conveniently. To view a list of activities (or sub-actions), expand the main action by double-clicking its associated icon or by clicking the small arrow to the left of the action. For more details, see Finding & Organizing Actions.

Once the desired activity is found, simply drag it onto the Steps panel or double-click it to make it a task step. In addition, the action itself can be dragged into the Steps panel. Doing so will display the properties dialog where an activity can be selected from a list. For more details, see Setting Action Properties.

> **NOTE:** Unlicensed actions and activities will appear opaque. Double-clicking, dragging or adding them to the Steps panel in any other way will generate an error.

Search dialog

The bottom portion of the Actions panel contains an intuitive search dialog that enables you to define search criteria and provide more efficient and effective searches. It supports dynamic search filtering, allowing you to enter all or part of an action's name and view only actions that contain matching text.

To find an action/activity

1. Click inside the Search dialog or press CTRL+SHIFT+F on your keyboard.
2. Enter all or part of an action's name. The list is updated as you type each letter. The list is updated as you type each letter.
3. To empty the Search dialog of its contents, do one of the following:
    - Click the "X" button located on the right side of the Search dialog (this button only appears when the Search dialog is populated with characters).
    - Press ESCAPE on your keyboard.

Context menu

By default, the Actions view displays all available actions in ascending alphabetical order and associated activities (or sub-actions) are hidden from view. Alternately, all actions can be viewed in descending alphabetical order and expanded to display all activities individually. All options that assist in locating and administering Automate Desktop actions as well as customizing the Actions panel are contained in a context menu that you can open by right-clicking a specific action or an empty portion inside the window Actions panel.

Item	Description
Add Step	Adds the selected action/activity to the Steps panel and automatically places it at the end of the task (for example, last step). This option is available only when a right-click is performed on a specific action/activity.
Insert Step	Inserts the selected action/activity directly above the currently highlighted step in the Steps panel. This option is available only when a right-click is performed on a specific action/activity.
Sort A to Z	Sorts the individual action folders in ascending or descending alphabetical order.
Expand All	Expands all categorized folders. This option is available only if the **Categories**option is enabled.
Collapse All	Collapses all categorized folders. This option is available only if the **Categories**option is enabled.
Add to Favorites	Adds the selected action to your **Favorites** list. This option is available only when a right-click is performed on a specific action.
Help (F1)	Opens the selected action's help topic. This option is available when a right-click is performed on a specific action. Selecting an action and pressing F1 also opens that action's help topic.

My actions view

Automate Desktop's array of structured actions and activities can automate virtually any type of business process one can think of. Nonetheless, most developers find themselves utilizing just a handful of activities specific to the needs of their business or department. The My Actions view allows easy access to such activities by way of Jump Lists. That way, you don't have to scroll through numerous actions or type a keyword in the Search bar to find an activity. Simply select the activity from the appropriate list in the My Actions panel. For additional details, see My Actions.

Favorites

The **Favorites** folder can be used as a placeholder for a collection of preferred actions and activities. Favorites can be created and managed by the user themselves. When an activity is defined as a favorite, a copy of that activity is added to the Favorites list. That way, users won't need to spend time searching through the long list of available actions. They can simply select the activity from their Favorites list. Users can also reorder their favorites by title or create folders/sub-folders to consolidate common favorites into specific categories, forming a more organized development environment. Actions and activities can be added to your favorites by way of the Actions panel or Steps panel. Once added, any favorites can be incorporated into task steps by way of drag and drop or by a double-click action.

To add an action or activity from the Actions Panel to Favorites

- Drag the desired action from the Actions panel onto the Favorites folder or any sub-folder.

  OR

- Right-click the desired action and select **Add to Favorites**from the context menu.

To add steps from the Steps Panel to Favorites

- Drag the desired steps from the Steps panel onto the Favorites folder or any sub-folder. To select more than one step, hold down CTRL during selection.

  OR

- Right-click the desired steps and select **Add to Favorites**from the context menu.

Snippets

For those who use specific activities that contain commonly used properties or settings, such activities can be saved in the **Snippets** folder. Snippets provide an easy way to implement frequently used code into a task. Instead of re-entering the properties for a specific activity or series of activities every time they're added as task steps, users can save existing steps as a snippet and simply drag and drop the snippet wherever it is needed in any task. A snippet can consist of one or more steps. Once a snippet is added to a task, its contents act as normal steps (that is, they can be reorganized or deleted or their properties can be modified as needed). Users can reorder their snippets list by title or create folders/sub-folders to consolidate common snippets, thus, creating a cleaner development environment.

To add one or more steps from the Steps Panel to Snippets

1. Drag the desired steps from the Steps panel onto the Snippets folder or any sub-folder or simply right-click the desired steps and select **Add to Snippets** from the context menu. To select more than one step, hold down CTRL during selection.
2. Enter a unique name for the new snippet.

> **NOTE:** Users will be able to save an unlicensed activity as a snippet and drag and drop that snippet into the Steps panel. However, once in the task panel, it should continue to behave as an unlicensed activity.

The **Recent** folder is populated with the most recently used actions and activities. The **Frequent**folder is populated with the most frequently used actions and activities. Similar to **Snippets** and **Favorites**, these folders are designed to make it easier and more convenient for you to find what you want by placing the actions and activities that you mostly use in a convenient location. By default, 10 items are displayed in the **Recent** and **Frequent**folders.

Context menu

Right-clicking an action located inside the **My Actions** panel will display a context menu with the following options.

Item	Description
Create Folder	Creates a folder at the current position. Allows you to better manage the actions and activities you use the most. This option is available only if a right-click is performed on an activity from your Favorites or Snippets list.

Item	Description
Remove	Removes the selected activity from its current position. This option is available only if a right-click is performed on an activity from your Favorites or Snippets list.
Reorder by Title	Reorders existing sub-items by title. Active only if a right-click is performed on a parent item.
Clear	Removes the selected activity or snippet from the My Actions panel.
Clear All My Actions	Clears the My Actions panel of all activities and snippets

Finding & Organizing Actions/ Activities

There are over 500 available actions and activities that you can use to create the steps of your task. This may seem overwhelming to some individuals, especially new or novice users. Therefore, the Task Builder provides a variety of ways to assist in easily finding actions or activities you are searching for. In addition, it keeps track of a user's favorite, most often and most recently used actions/ activities and places them in the My Actions panel for quick and easy access.

Finding actions & activities

The bottom portion of the Actions panel contains an intuitive search dialog (highlighted in red below) that enables you to define search criteria and provide more efficient and effective searches. It supports dynamic search filtering, allowing you to enter all or part of an action's name and view only actions that contain matching text. The list is updated as you type each letter.

To search for an action or activity

1. Click inside the search dialog or press CTRL+ SHIFT + F to automatically place the cursor inside the dialog.
2. Type all or part of the action name you want to search for. The list of relevant actions narrow as you type each letter.
3. Use the UP or DOWN arrows to navigate to the desired action then press ENTER or click and drag the action to the Steps pane.
4. To clear the search, click "X" located on the right side of the search dialog or press ESC.

Organizing actions & activities

By default, actions are categorized in ascending alphabetical order and activities (or sub-actions) are categorized in a logical sequence. Alternately actions can be viewed in descending alphabetical order or they can be expanded to reveal all activities. Most commands and operations relevant to actions are contained in the **Actions**tab of the ribbon (as shown below).

To change the sort order of actions

1. Right-click anywhere in the Actions panel and select the context menu item labeled **Sort A to Z**. The order is changed to ascending or descending alphabetical order (depending on the original sort order).
2. Repeat step 1 again to switch back to the previous sort order.

> **NOTE:** Sorting only applies to actions. They don't apply to activities which are ordered in a fixed logical sequence.

To expand or collapse actions

1. To expand the actions list, revealing the list of activities for each action (if any), do one of the following:
    - On the ribbon, select the **Actions** tab and click the **Expand All**button.
    - Right-click anywhere in the Actions panel and select the context menu option **Expand All**.
2. To collapse the actions list, do one of the following:
    - On the ribbon, select the **Actions** tab and click the **Collapse All**button.
    - Right-click anywhere in the Actions panel and select the context menu option **Collapse All**.

My Actions

Having quick access to common items is essential for a productive work environment. Task Builder supports this capability with the My Actions pane. Similar to Jump Lists in Windows that enable quick access to frequently and recently used items, My Actions can take you right to the actions and activities you turn to each day. **The My Actions pane is designed** to make it easier for you to access common actions or recently used activities quicker by conveniently placing them in common folders directly above the Actions view (circled below).

You can use My Actions to open actions/activities, and you can also "pin" favorites, so you can quickly get to the actions that you use every day. You can drag an action from one of the folders in My Actions directly to the Steps panel. In addition, you can save actions that contain common properties as "snippets." Snippets store the current properties set for the action so yo can reuse it in different tasks.

The My Actions view houses four types of items:

- Favorites
- Snippets
- Recent/frequent

Favorites

Favorites can be used as a placeholder for a collection of preferred actions and activities. When an activity is set as a favorite, a copy of that activity is added to the **Favorites**folder located in the Actions panel (highlighted in red below). That way, users spend less time searching through the long list of available actions and activities. They can simply select the activity from their Favorites list. Individual folders can be created to consolidate common activities into specific categories, forming a more organized development environment.

> **NOTE:** You can add actions and individual activities to your favorites list. By default, the list is set in chronological order, starting with the earliest addition and following the order in which they occurred. However, you can resort the list in alphabetical order by right-clicking **Favorites**and selecting **Reorder by title**.

To set an action or activity as a favorite

1. In the Actions panel, navigate to the action or activity you wish to add to your favorites list (only one action/activity folder can be selected at a time).
2. Right-click the action/activity and select **Add to Favorites** from the context menu that appears.

In addition, you can select the steps that perform the activity you wish to add to your favorites in the Steps panel. To select more than one step, hold down CTRL during selection, and then right-click the steps and select **Add to Favorites** from the context menu that appears.

To add a folder/sub-folder to Favorites

1. In the Actions panel, right-click **Favorites**and select **Create Folder**. A new folder is added to your favorites list.
2. Rename the newly created folder to the desired name.
3. Add sub-folders under the newly created folder by right-clicking that folder, and then selecting **Create Folder**.
4. Add actions/activities to a folder under **Favorites**by clicking and dragging them into the folder of your choice.

To remove actions, activities, or folders from Favorites

1. In the Actions panel, under **Favorites**, select the action, activity, or folder you wish to remove (only one action/activity/folder can be selected at a time).
2. Right-click the action/activity and select **Remove**.
3. To clear **Favorites**of all items (including actions, activities and folders), right-click on **Favorites** and then select **Clear**from the context menu that appears.

Snippets

For those who use common activities that perform identical operations in many tasks, such activities can be saved as snippets. Snippets provide an easy way to implement frequently used steps into a task. Instead of re-entering the properties for a specific activity or series of activities every time they're added as task steps, you can save the steps as a snippet and simply drag and drop the snippet wherever it is needed in any task. The main idea is to make the process of reusing as easy as possible to avoid wasting your valuable time to enter the same properties again.

A snippet can consist of one or more task steps that perform common actions. For example, a developer may create a basic Input - Send keystrokes snippet to enter specific keys when a user opens a particular window or clicks a specific button. Other snippets might be used to perform Dialog - Open file and Dialog - Save file operations.

Once a snippet is added to a task, its contents act as normal steps (that is, they can be reorganized or deleted or their properties can be modified as needed). Task steps can be easily saved as a snippet by way of drag-and-drop. Sub-folders can be added to the Snippets folder so developers can easily organize common or related snippets into categories, creating a cleaner, more manageable development environment.

> **NOTE:** Users will be able to save an unlicensed activity as a snippet and drag and drop that snippet into the Steps panel. However, during Runtime, the unlicensed step will fail, generating an "unlicensed" error.

To add one or more steps to snippets

1. Highlight the desired steps from the **Steps**panel. To select more than one step, hold down **CTRL**during selection.

   > **NOTE:** Selected steps do not need to be sequential.

2. Right-click on the selected steps, and then select **Add to Snippets**.

To add a folder/sub-folder to snippets

1. Right-click on **Snippets**, and then select **Create Folder**. A new folder is added to your favorites list.
2. Rename the newly created folder to the desired name.
3. Add sub-folders under the newly created folder by right-clicking that folder, and then selecting **Create Folder**.
4. Rename the newly created sub-folder to the desired name.

Recent and Frequent Lists

Task Builder automatically saves a history of recently and frequently used actions and activities, and displays them in Jump Lists under the **Recent** and **Frequent**folders (shown below) so you can easily "jump" to these items with a click of a button. The lists are automatically populated based on how frequently and how recently items have been used. For example, if the last activity you opened or used in a task was a VMWare Guest - Delete file activity, the next time you open Task Builder, this activity will be contained in your **Recent**folder, and possibly, your **Frequent**folder as well, depending on how often you used the activity in the past. By default, the **Recent** and **Frequent** folders are populated with up to 10 entries.

Having access to frequent and recent lists is great if you want quick access to often used and popular actions and activities without having to browse in the Actions list or perform a search, but not great if you're a privacy freak who doesn’t want someone random to see what kind of actions/activities you often use if, for example, you use a shared or public computer, or you may just want to clear this history periodically as a security measure. Task Builder makes it easy to clear your recent and/or popular list of actions/activities or clear all Jump List items altogether.

> **NOTE:** Clearing **Jump List** items removes items from your **Recent**and **Frequent** lists. It doesn’t delete the items from your computer permanently.

Action Properties

A major point of task construction is entering the properties required for each of the actionsto be included as task steps. Accessing an action's properties can be can be accomplished within the Task Builder in a number of ways:

- Dragging an action from the Actions panel and dropping it into the Steps panel.
- Double-clicking an action from the Actions panel or right-clicking the action and selecting **Add step** or **Insert step** from the context menu.
- Double-clicking an existing step from the Steps panel or right-clicking the step and selecting **Properties** from the context menu.

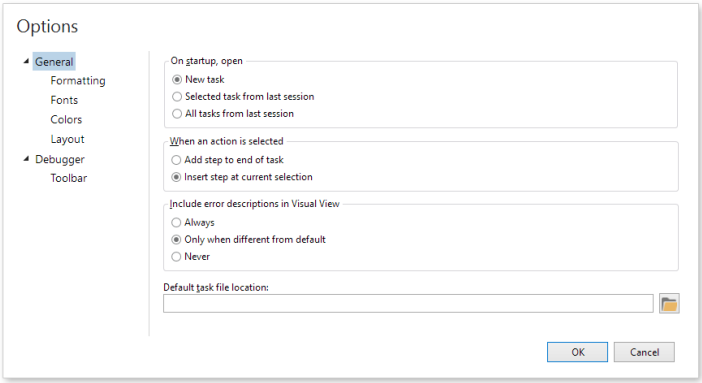
A dialog window appears titled Action Properties (also known as the Action Editor) displaying the selected activity's properties categorized into separate tabs. The left portion of the editor contains the full list of consolidated activities common to a given action. This enables jumping from one activity to another without the need to re-enter required parameters or re-open the action editor.

Depending on the action being edited, certain parameters may need to be entered or validated in order to properly add the action to the Steps panel. After the properties are set and the proper parameters assigned, clicking the **OK** button saves the settings and closes the properties dialog. The action then becomes a step and its settings are then displayed in the Steps panel.

> **NOTE:** Information regarding the properties and parameters available for any given action can be accessed in the Task Builder by clicking the **Action icon** or pressing F1.

Task Builder Options

The Task Builder contains its own set of options which can be configured to meet a user's specific necessities. They include color, icon and font settings, viewing options, debug preferences and formatting properties. Task Builder options can be accessed by way of **File**> **Options**.



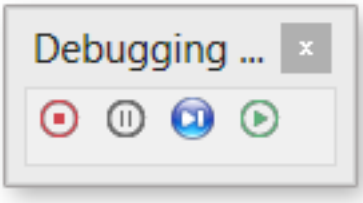
Available Options

Task Builder options are grouped into six separate categories, each encompassing specific preferences and options. Below lists the available categories, with links to the topics covering each.

Option	Description
Color Options	Contains options that determine the color to be used for the Task Builder interface or allows adjustments to be made to the current color scheme.
Debugger Options	Contains options that affect Task Builder's behavior while running and debugging tasks.
Fonts Options	Contains options to modify the font name, size and style to be used for the Visual view and the AML view.
Formatting Options	Contains options that deal with how steps should be formatted in the Steps pane.
General Options	Contains options that determine certain behavioral characteristics of Task Builder. Also determines the default managed task location.
Layout Options	Contains an option to reset Task Builder back to its original (default) layout.
Toolbar Options	Contains options that determine the look and feel of Automate's debugger toolbar.

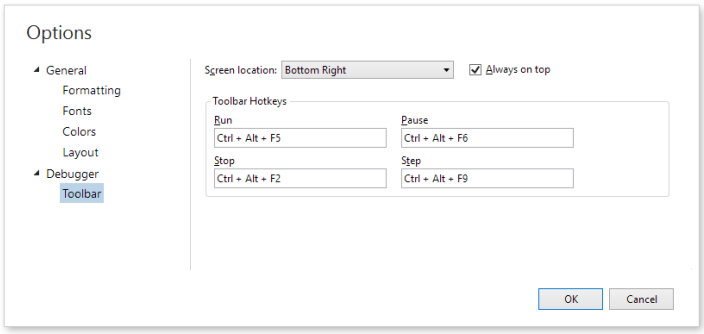
Task Builder Toolbar Options

The Debug toolbar (illustrated below) is a small floating window that appears when a task is run from the Task Builder. It contains buttons to stop, pause, re-run and step through an active task to further aid you during the development stage. The Debug toolbar automatically closes upon completion of a running task or you can close it at any time by clicking "x".



The Debug toolbar supports hot-keys (also known as shortcut keys) that can be used as an alternate control mechanism. You can change the default toolbar shortcut keys to any desired key combinations not already in use, and you can change the position of the Debug toolbar on the screen. In addition, you can choose to show or hide the Debug toolbar or have it always appear in the foreground or background.

To access the Toolbar Options page in the Task Builder, select **File**> **Options** > **Debugger** > **Toolbar**. Toolbar options is a subset of Task Builder Options.



Parameters

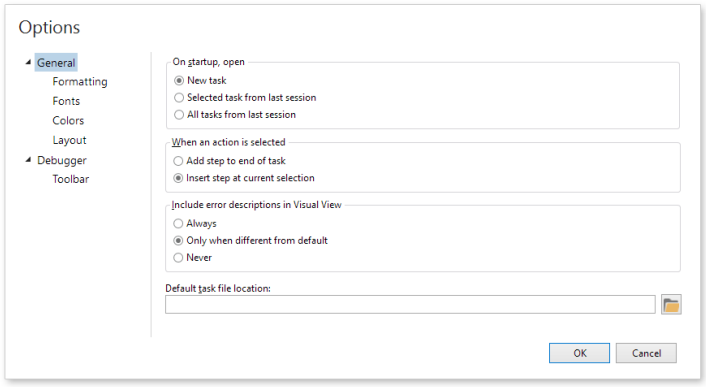
The following table describes available Toolbar options:

Property	Default	Description
Screen Location	Bottom Right	Specifies the area on the screen that the debug toolbar should be displayed. The available options are: • **Do not show** -The debug toolbar will not appear during task execution. • **Top Left**- The debug toolbar will be displayed on the upper left corner of the screen. • **Top Right** - The debug toolbar will be displayed on the upper right corner of the screen. • **Bottom Left:** - The debug toolbar will be displayed on the lower left corner of screen. • **Bottom Right** - The debug toolbar will be displayed on the lower right corner of screen.
Always on Top	Enabled	If enabled, the toolbar will always be in the foreground, in front of other windows. If disabled, the toolbar will appear in the background. This parameter is enabled by default.
Toolbar Hot-keys	• Run: CTRL+ALT+F5 • Stop: CTRL+ALT+F2 • Pause: CTRL+ALT+F9 • Step: CTRL+ALT+F6	Allows entry of specific shortcut keys (also known as hot-keys) used to run, stop, pause or step through a task. The available options along with their default hot-key parameters are as follows: • **Run**- Runs the entire task, from beginning to end, or until an error is encountered. • **Stop**- CTRL + ALT + F2 • **Pause**- CTRL + ALT + F9 • **Step**- Runs the task step by step, pausing on each step. **NOTE:** For more details about using the various run options in Task Builder as a debug tool, see Run Options.

Task Builder General Options

Task Builder contains general options that enables control over a variety of interactive aspects. You can choose whether double-clicking an action/activityfrom the Actions panel should add it to the beginning or end of the task. Also, you can dictate what task should appear the next time the Task Builder is open, whether it be a new task, all tasks from the previous session or selected task from the previous session.

The Task Builder **General Options** page can be accessed by navigating to **File** > **Options** > **General**. General options is a subset of Task Builder Options.



Parameters

The following table describes Task Builder's available General options:

Property	Default	Description
On startup, open	New task	Dictates the Task Builder's startup behavior. This option is relevant only when the Task Builder is started manually from Windows Start menu or by the executable file by way of Program Files directory (for example, `C:\Program Files (x86)\Automate Desktop2024\AMTB.exe`). The previous task is never opened when Task Builder is started for a managed task through Task Administrator. • **New task** - A new task will open. Previously opened tasks are ignored. • **Selected task from last session** - Automatically re-opens the task that was last open in the Task Builder. If multiple tasks were previously open, the active/selected task is the one that will re-open. • **All tasks from last session** - Automatically re-opens all tasks that were previously open.

Property	Default	Description
When an action is selected	Add step to end of task	When double-clicking an action from the Actions panel, determines where that action is inserted in the Steps panel. The available options are: • **Add step to end of task** - The action is automatically inserted in the Steps as the last step. • **Insert step at current selection**- The action is automatically inserted in the Steps panel directly where the currently selected (highlighted) step is positioned. The current step and all others below it are moved a single step downward. **NOTE:** In either case, a new step can be inserted at the desired position by dragging the action from the Actions panel onto the desired position in the Steps panel instead of double-clicking it.

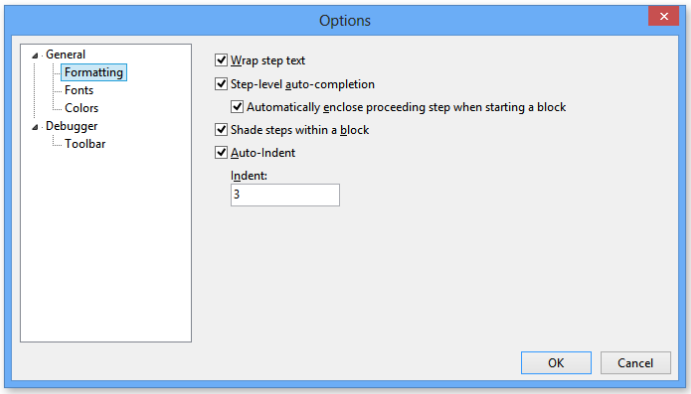
Property	Default	Description
Include error descriptions in Visual view	Only when different from default	Controls when the Visual view (as opposed to AML view) in the Steps panel displays descriptive text about each step's error handling along with descriptive text about the step itself. Every Automate Desktop step performs default error handling if the step fails. Select from the following: • **Always** - Always appends the error handling description to each step. This can cause extra, redundant text to be displayed in the Steps pane. • **Only when different from default** - Appends descriptive text about the step's error handling only when an error handling option has been set that is different from the default. This will cause the error description to be omitted in the majority of cases because the default error handling is sufficient for most steps (selected by default). • **Never** - Never appends the error handling description. The error handling can only be viewed by opening the properties dialog for the step.

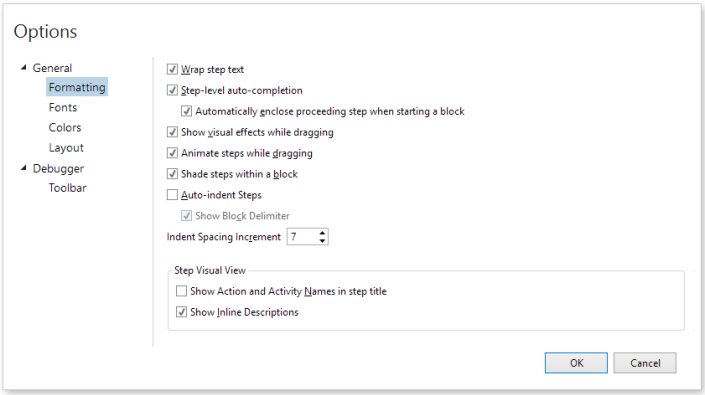
Property	Default	Description
Task Builder auto save options	Disabled	If selected, the **Automatically save task(s) every 2 minutes** option will automatically save tasks with an associated file every 2 minutes. **NOTE:** After selecting or clearing this setting, Task Builder must be restarted before changes will take effect.
Default task file location	C:\Users\<user.name>\Documents\Automate Desktop2024 Tasks	By default, unmanaged tasks are saved to a location accessible by the user that initially installed the program. This location is different from the default managed task location and may vary depending on the operating system. To indicate the default location to which an unmanaged task should be saved, click the folder icon to browse available folders to select from or enter the full path to the folder in the provided text box. **NOTE:** If specifying a network location as the default task location, it is critical that mapped drive letters not be used. Folders should always be specified using UNC (Universal Naming Convention) paths. For example: `X:\pathname\` should be `\\servername\pathname\`. This is because mapped drives are available only when a user logs on and this does not occur for LocalSystem services.

Task Builder Formatting Options

Task Builder formatting preferences allow you to modify how activities that represent a block of steps, such as steps inside a Loop or If statement, are formatted in the Steps panel. You can choose to automatically add closing steps to those that require one (for example, Loop step should automatically be followed by an End Loop step) or you can choose to add closing steps manually as you construct the task. You can also decide upon whether those blocks of steps should be indented and what the indentation value should be.

To access the Formatting Options page, from Task Builder, select **File**-> **Options** -> **Debugger** -> **Formatting**. Formatting options is a subset of Task Builder Options.





Parameters

The following table describes Task Builder's available Formatting options.

Property	Default	Description
Wrap step text	Enabled	If enabled, the text that appears in the Steps panel will automatically wrap itself so as not to run off the right edge of the window. This enables all text to be viewed without the need to scroll to the right. If disabled, the text that appears in the Steps panel will run off the right edge.
Step level auto-completion	Enabled	If enabled, any activity added to the Steps panel that starts a block of steps will be followed by the activity used to end the block. For example: • If enabled, any If statement will automatically be followed by an End If step. If disabled, you must manually add an End If step. • If enabled, any Loop step will automatically be followed by an End Loop step. If disabled, you must manually add an End Loop step. • If enabled, any Case statement will automatically be followed by an End Case step. If disabled, you must manually add an End Case step. **NOTE:** An activity can be added from the Actions panel onto the Steps panel by way of a double-click or drag-and-drop operation. If using drag-and-drop to add your steps, setting the Task Builder General Option titled **When an action is selected**to **Add step to end of task** will make this option irrelevant because all activities that are added by way of double-click action will automatically be added as the last step of the task.
Automatically enclose proceeding step when starting a block	Disabled	If enabled, the proceeding step is automatically enclosed between the newly inserted block of steps. If disabled, no steps will be enclosed between the start and end block. This option is available only if the **Step level auto-completion**option is enabled.
Show visual effects while dragging	Enabled	If enabled, a visual overlay of the item being dragged along with a red line will be displayed in the Steps panel to determine the drop location. If disabled, only a red line will be displayed during a drag and drop operation.

Property	Default	Description
Animate steps while dragging	Enabled	If enabled, a drag and drop operation performed in the Steps panel will animate all affected steps to show the user how those steps would change position in response to the current operation. For example, when you drag an activity between two steps, they will move apart to make room for the drag source. If disabled, no animation will be applied to other steps during a drag and drop operation.
Shade steps within block	Enabled	If enabled, any steps contained between the start and end of a block of steps will be shaded. If disabled, no shading will be applied to any steps contained within a block of steps.
Auto-indent Steps	Enabled	If enabled, allows steps to be automatically indented. The default indent value can be entered in the **Indent Spacing Increment** parameter below.
Show Block Delimiter	Enabled	If enabled, a vertical line will be displayed to specify the start and end of a block of steps. If disabled, no delimiter will be shown. This option is active only if the **Auto-indent steps** option above is enabled. > **NOTE:** Delimiters only appear when the block of steps are in expanded view. They are hidden in collapsed view.
Indent Spacing Increment	7	Specifies the indentation value. This parameter is set to 5 by default and only available if the **Suggest Indent** parameter is enabled.

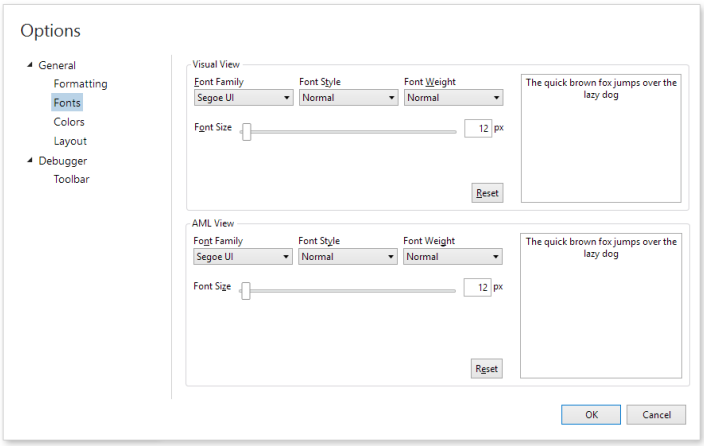
Step Visual View Parameters

Property	Default	Description
Show Action and Activity Names in step title	Disabled	If enable, each step in the Steps panel will display its designated action and activity name. If disabled, no action and activity name will be displayed. > **NOTE:** If the action and activity name is not displayed, a step can still be recognized by its unique icon and inline description (if these options are enabled).
Show Inline Descriptions	Enabled	If enabled, an inline description of what the step will perform will be included. If disabled, no description will appear.

Task Builder Font Options

Task Builder font options allow customization of fonts (that is, font family, style, weight and size) to be displayed in the Steps Panel when the task is set to either Visual view or AML view.

To access Task Builder's Font Options page, navigate to **File** > **Options** > **General** > **Fonts**. Font options is a subset of Task Builder Options.



Parameters

The following table describes available font properties, as well as their Visual and AML defaults values. To reset all values to default, click the **Reset** button.

Property	Visual/AML	Description
Font Family	Segoe UI/Courier New	The name of the font to be used when Visual mode is selected from the View menu. An easy to read font for this view is suggested, such as Segoe UI or Tahoma, since Visual mode is meant to provide a clear, natural-language description about the task's steps.
Font Style	Normal/Normal	The style of font to be used. The available options are: • **Normal** - The text is shown normally. • **Italic** - The text is shown in italics. • **Oblique** - The text is "leaning" (oblique is very similar to italic, but less supported).

Property	Visual/AML	Description
Font Weight	Normal/Normal	The weight of the font (or the thickness of the character outlines relative to their height). The available options are: • **Light** - Defines lighter or thinner characters. • **350** - Defines characters with weight class between **Light** and **Normal**. • **Normal** - Defines normal characters. • **SemiBold** - Defines semi-thick characters. • **Bold** - Defines thick characters. • **Black** - Defines thicker characters.
Font Size	12 pixels/12 pixels	The font to be used when AML mode is selected from the View menu. A fixed-width font, such as Courier New, for AML view is suggested, since this type of view is typically used for fine, programmatic refinements to task steps.

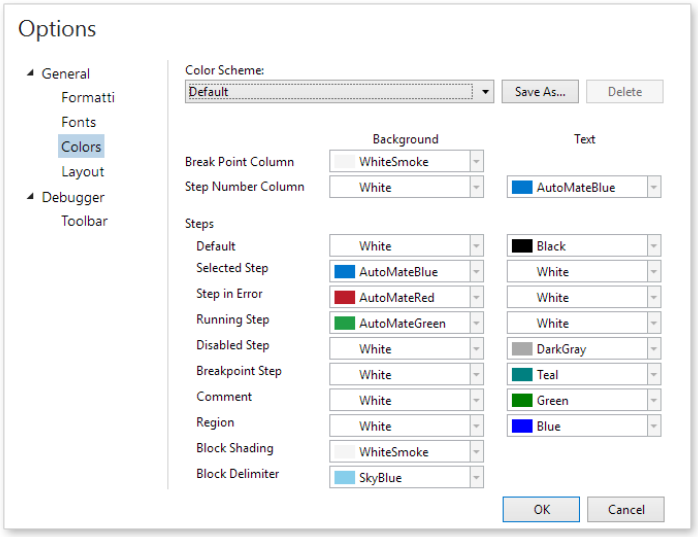
Task Builder Color Options

Task Builder's Steps panel can be configured to use a predefined color scheme or you can fully customize the collection of colors used to represent the steps of your task and save it as your own personal color scheme. A color scheme allows different users of Task Builder to create their own custom "look and feel" when creating, editing and debugging tasks. When saving a custom color scheme, that color scheme becomes your default scheme and is available only to you.

To access the color Options page, from Task Builder, select **File**> **Options** > **General** > **Colors**. Color options is a subset of Task Builder Options.

Parameters

The following table describes elements in the Steps panel that text and background colors apply to along with text and background colors that are set as default.



Property	Background	Text	Description
Color Scheme	---	---	Indicates the combination of colors to be applied to text and background elements that appear in the Steps panel. To create your own custom color scheme, select a color for each element, click **Save As** and enter a name for the new scheme. To delete a custom color scheme, select it from the drop-down list and click **Delete**. You can also select from a list of pre-defined color schemes which are as follows: • **Default** - The default color scheme used in Automate Desktop 2024. • **Automate 10** - The default color scheme used in Automate 10. • **Automate 9** - The default color scheme used in Automate 9. • **Automate 6** - The default color scheme used in Automate 6. • **Automate 5** - The default color scheme used in Automate 5. • **Plain** - A color scheme made up of basic colors. **NOTE:** Only custom color schemes can be edited or deleted. To create a custom color scheme, you must first use the **Save As** option to save a copy of any original scheme.
Breakpoint Column	White Smoke	---	The background color of the column that contains Breakpoints. This is the left-most column in the Steps panel.
Step Number Column	White	Automate Blue	The text and background color of the column that displays step numbers. This column appears along the right side of the Breakpoints column, which is the left-most column in the Steps panel.

Property	Background	Text	Description
Default	White	Black	The text and background color for each default line of text that appears in the Steps panel. A step that does not fit the characteristics of any properties described below would be considered default.
Step Expression	---	Orange	The text color of a step expression.
Selected Step	Automate Blue	White	The text and background color of one or more steps that are currently selected (highlighted).
Step in Error	Red	White	The text and background color of a step that caused an error. When debugging a task from Task Builder, this color combination will appear in the Steps panel for a step that throws an error.
Running Step	Green	White	The text and background color of the step that's currently running. This color combination allows easy tracking of step by step execution while debugging a task.
Disabled Step	White	Gray	The text and background color of a disabled step. Disabled steps are not executed at runtime.
Breakpoint Step	White	Teal	The text and background color of any step that contains a Breakpoint. For debugging purposes, when a task is run from Task Builder, execution pauses at any step defined with a breakpoint.
Comment	White	Green	The text and background color of any step that contains a Comment. In Automate Desktop, comments provide a means for adding remarks or placing notes into your task. A comment is not an action or activity, therefore, it is skipped during runtime.

Property	Background	Text	Description
Region	White	Blue	The text and background color of any step that signifies the start and end of a Region. **NOTE:** This only applies to expanded regions. When a region is collapsed, the step that marks the start of the region only appears. The remainder of steps, including the one that marks the end of the region are hidden.
Block Shading	White Smoke	---	When selecting the first step in a block of steps (for example, Loop blocks, If Statements, Regions) this background color signifies the steps contained in the block, up to and including the last step. **NOTE:** This only applies to expanded regions. When a region is collapsed, the step that marks the start of the region only appears. The remainder of steps, including the one that marks the end of the region are hidden.
Block Delimiter	Sky Blue	---	The color of the delimiter line used to signify a block of steps, including the first and last step. **NOTE:** This only applies to expanded regions. When a region is collapsed, the step that marks the start of the region only appears. The remainder of steps, including the one that marks the end of the region are hidden.

To switch color schemes

1. In the **Color Scheme** parameter, click the drop- down combo box and select the desired scheme from the list that appears.
2. The selected scheme's name appears in the **Color Scheme** parameter and automatically becomes the default scheme.
3. Click **OK** to save changes.

To create a custom color scheme

1. Create a copy of the default color scheme or any existing scheme by selecting it from the **Color Scheme** parameter's drop-down list and clicking **Save As...**.
2. Enter a new name in the dialog that appears and click **OK**. The new scheme you created is automatically saved as the default color scheme.
3. Select the desired color for each text and background elements.
4. Click **OK**to save changes.

> **NOTE:** The default color scheme or any existing ones that appear in the **Color Scheme** parameter's drop-down list are not customizable. You must first create a copy of one of the existing schemes in order to customize it.

To delete a custom color scheme

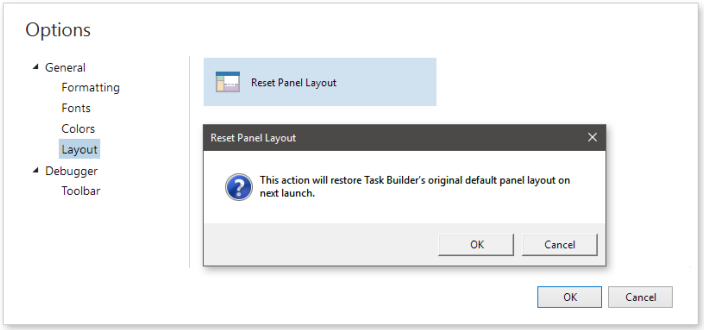
1. In the **Color Scheme** parameter, click the drop-down arrow and select the name of the custom scheme you wish to delete, then click **Delete**.
2. A dialog appears verifying whether or not to delete the custom color scheme. Click **Yes**to complete the operation.

> **NOTE:** The default color scheme or any existing pre-defined color schemes that appear in the **Color Scheme** parameter's drop-down list cannot be deleted. Only custom color schemes are allowed to be deleted.

Task Builder Layout Options

Task Builder's interface is customizable in ways that enable users to drag and dock certain panels wherever they please, unpin docked panels to enter an auto-hide state, and float panels separately. The Layout Options page lets you reset Task Builder's panels back to its original design on the next launch.

To access Task Builder Layout options, navigate to **File** > **Options** > **General** > **Layout**. Layout options is a subset of Task Builder Options.



To reset Task Builder the default layout

1. From the Layout section, click **Reset Panel Layout**.
2. A pop-up window informs you that Task Builder's original default panel layout will be restored on the next launch. Click **OK** to complete the operation. At this point, you must close all open instances of Task Builder. Thereafter, any new instance of Task Builder will display its original panel layout.

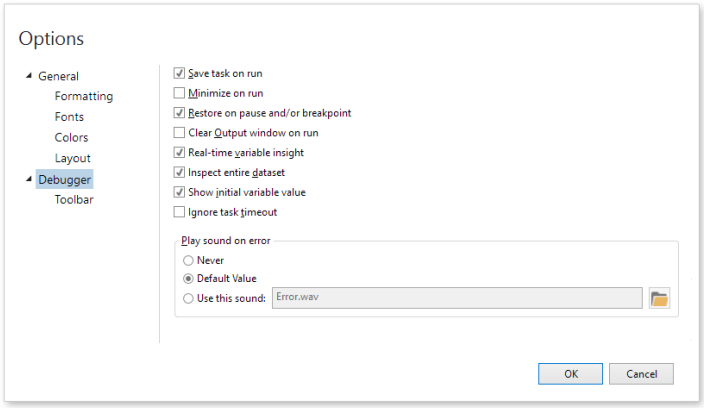
> **NOTE:** If you change your mind, you can always cancel the reset layout operation before closing Task Builder by returning to the Layout section and clicking **Cancel Reset Panel Layout.**

Task Builder Debugger Options

The Task Builder includes settings that affect its behavior while running a task. In some cases you may want to change these settings to better fit your debugging needs. For instance, you can opt to minimize the Task Builder window during execution to better examine an interactive task, automatically clear the Output Debug Panel after each run, or play a custom sound when an error occurs.

To access Task Builder's Debugger Options page

- Click to **File> Options>Debugger**. Debugger options is a subset of Task Builder Options.



Parameters

The following table describes available Debugger options:

Property	Default	Description
Save task on run	Disabled	If enabled, Task Builder automatically saves changes made to a task when clicking the **Run**button. If the task has not been saved yet, Automate Desktop will prompt the user whether or not to save before running. If disabled, changes will not be saved upon run.
Minimize on run	Disabled	If enabled, Task Builder minimizes to the system tray when execution starts. When the task ends, Task Builder restores itself onto the desktop and highlights the current step or displays **Finished** as the step status in the status bar. If disabled, Task Builder stays on the desktop (does not minimize or hide itself) during task execution. **NOTE:** It is recommended to enable this option when testing tasks that include interactive steps (for example, Send Keystrokes, Move Mouse to Object actions) or steps that interact with other windows (for example, Maximize Window, Minimize Window actions). This is due to leaving the Task Builder window on the desktop may interfere with other windows that appear during runtime. Doing so may result in a Send Keystrokes step, for example, failing to send keystrokes to the proper window or application.
Restore on pause and/or breakpoint	Enabled	If enabled, when task execution is manually paused (when a user clicks the **Pause**button) or pauses at a breakpoint, and the Task Builder window is currently minimized, it restores itself and highlights the current step. When execution continues, the Task Builder window, once again, minimizes to the system tray.
Clear Output window on run	Enabled	If enabled, clears the contents of the Output window before each task execution . If disabled, new debugging output will append existing output accumulated from previous runs.
Limit entries in output panel to	Disabled	If enabled, limits the number of entries in the Output panel to the numeric value entered here. Once the value is exceeded, the oldest entry is deleted. If disabled, entries are not limited.

Property	Default	Description
Real-time variable insight	Enabled	If enabled, the Variables window is updated after each step to show the current value of existing variables on a step by step basis. If disabled, the Variables window is updated only when the task ends or when it is in a paused state (by clicking the **Pause**button, when a Breakpointis encountered or while stepping through with the use of the **Step** button). **WARNING:** Enabling this option could cause Task Builder to run tasks slower.
Inspect entire dataset	Disabled	If enabled, during runtime, extended dataset properties that are normally hidden (for example, creation date/time, total rows) will be displayed in the Variable window. If disabled, only basic dataset properties will be displayed. **WARNING:** Enabling this option could cause Task Builder to run tasks slower.
Show initial variable value	Enabled	If enabled, causes the Variables window to include a column for **Initial Value** in addition to the **Current Value** column. If disabled, only the current value is shown.
Play sound on error	Error.wav	Denotes whether to play a sound when the task stops as a result of an error. The selections are: • **Never** - Do not play a sound when an error occurs. • **Use default sound** - Use the default system error sound, as specified in Window's Control Panel. • **Use this sound** - Specify a valid path and file name of a .wav file to use.

Task Builder Ribbon

The ribbon is a contextual interface designed to increase efficiency and make it easier for users to find features and quickly access popular commands and controls during task construction. The ribbon spans the top of Task Builder, directly below the title bar. It is filled with graphical representations of control elements which are grouped by different functionality. Commands are organized in logical groups, which are collected together under operation related tabs. The ribbon brings the most common commands to the forefront, in plain sight, so you no longer have to roam aimlessly through the clutter of menus, sub-menus, and toolbars searching for what you want.

Enlarging or maximizing the Task Builder window auto-expands the ribbon vertically. To add additional space, the ribbon can be collapsed so only the tabs appear. This can be accomplished by clicking the **Pin/Unpin Ribbon** button. Since not every single option will fit on the ribbon, drop-down menus are available which are represented by small arrows below certain buttons/commands. Clicking such arrows displays a drop-down menu which contain related sub-commands. For example, if you click the arrow below the **Run** icon, a drop-down menu will appear displaying related commands such as **Run All**, **Run Selected**, **Run From Here**, and **Step** (shown below).

Tabs and Commands

The Task Builder ribbon is categorized into three contextual tabs, **File**, **Home**, and **Actions**. Each represents an activity area grouped together with related commands, controls or buttons that represents the operation to perform. To view a description of each command and associated hot-keys (if any), hover the mouse cursor directly above the desired command. The following tables describe the available commands contained within each tab.

Home Tab Commands

The following table details each command found in the ribbon's **Home** tab along with their associated controls and keyboard hot-key combinations (if applicable). Each command is categorized by the group they reside in.

Group	Command	Description	Hot-Key
Document	Save and Close	Saves the current task and closes the Task Builder window.	ALT+ SHIFT + A
	Save Copy As...	Saves a copy of the task as an AML (Automate Desktop Markup Language) file.	CTRL + SHIFT + S

Group	Command	Description	Hot-Key
Clipboard	Cut	Cuts the selected steps. To select multiple steps, hold down CTRL during selection. To select all steps, press CTRL+A or click from the Find group. More on copying reusing task steps	CTRL + X
	Copy	Copies the selected steps to the clipboard. To select multiple steps, hold down CTRL during selection. More on copying & reusing task steps	CTRL + C
	Copy Description	Copies the text description of the selected steps. The description can then be pasted into another document such as Notepad. To select multiple steps, hold down CTRL during selection. More on copying & reusing task steps	CTRL + D
	Paste	Pastes the previously copied or cut steps. The stepss are pasted directly below the currently highlighted line in the Steps pane. More on copying & reusing task steps	CTRL + V
	Delete	Deletes the selected steps. To select multiple steps, hold down CTRL during selection.	(DEL)

Group	Command	Description	Hot-Key
Find	Find	Finds a specific word or phrase within the task. More on Find & Replace	CTRL + F
	Find Next	Finds the next instance of a word or phrase. More on Find & Replace	F11
	Find Previous	Finds the previous instance of a word or phrase. More on Find & Replace	F12
	Replace	Replaces an occurrence of the selected text string. More on Find & Replace	CTRL + H
	Replace Next	Replaces the next occurrence of the selected text string. More on Find & Replace	CTRL + SHIFT +R
	Select All	Selects all steps included in the Steps panel.	CTRL + A
	Select Step Number	Opens a dialog allowing entry of the desired step to select. Mainly used to quickly navigate to a specific step within a task that includes a significantly large amount of steps.	CTRL + G
	Select Label	Opens a dialog allowing entry of the desired label to go to. Used to jump to another section of the task defined by a Label.	CTRL + L
Layout	Step numbers	Turns step numbers On/Off as they appear on the Steps pane (On by default). More on editing task steps	---
	Word Wrap	Turns word wrap On/Off. When set to ON, the text becomes wrapped in the Steps pane so it doesn't scroll across the entire screen (On by default). More on editing task steps	---
	Panel Layout	Shows/Hides specific Task Builder windows. All windows are shown by default.	---

Group	Command	Description	Hot-Key
Task	Run	Runs the steps of the current task sequentially. More on run options	F5
	Run Selected	Runs the selected steps. More on run options	CTRL + F5
	Run from Here	Runs all steps from the specified step onward. More on run options	SHIFT + CTRL + F5
	Step	Runs the task one step at a time starting from the highlighted step. Click this button each time you want to run the next step. More on run options	CTRL + F2
	Pause	Pauses a running task. More on run options	F6
	Stop	Stops and resets a running task. More on run options	CTRL + F2

Group	Command	Description	Hot-Key
Step	Edit	Opens the properties of the selected step for editing.	---
	Up Arrow	Moves the selected steps up one line. To select multiple steps, hold down CTRL during selection. More on editing task steps	CTRL + UP
	Down Arrow	Moves the selected steps down one line. To select multiple steps, hold down CTRL during selection. More on editing task steps	CTRL + DOWN
	Left Arrow	Decreases indentation of the selected steps. To select multiple steps, hold down CTRL during selection. More on editing task steps	CTRL + LEFT
	Right Arrow	Increases indentation of the selected steps. To select multiple steps, hold down CTRL during selection. More on editing task steps	CTRL + RIGHT
	Create Region	Creates a region. More on Regions	CTRL + R
	Encapsulate in Region	Encapsulates any selected steps into a region. More on Regions	CTRL + E
	Rename Region	Renames the selected region. More on Regions	---
	Clear Region	Clears the selected region. More on Regions	---
	Clear All Regions	Clears all regions. More on Regions	---
	Expand All Regions	Expands all regions. More on Regions	CTRL + SHIFT + E
	Collapse All Regions	Collapses all regions. More on Regions	CTRL + SHIFT + C
	Reset Indent	Removes indentation from a step. More on editing task steps	---

Group	Command	Description	Hot-Key
	Disable	Enables/Disables execution of the selected steps. To select multiple steps, hold down CTRL during selection. Disabled steps appear grayed out and are ignored during task execution. Newly added steps are enabled by default.	---
	Bookmark	Adds a bookmark to the selected steps. To add to multiple steps, hold down CTRL during selection. Bookmarks are a means of marking steps so you can find them easily when constructing or editing a task. More on bookmarks	CTRL + F3
	Next Bookmark	Goes to the next step that contains a bookmark. More on bookmarks	F3
	Previous Bookmark	Goes to the previous step that contains a bookmark. More on bookmarks	SHIFT + F3
	Breakpoint	Adds a breakpoint to the selected steps. To add a breakpoint to multiple steps, hold down CTRL during selection. A breakpoint is a debug tool that pauses task execution at the specific step to allow the developer time to examine particular data that may change during the course of the task (for example, variables or datasets). More on Breakpoints	F8

Group	Command	Description	Hot-Key
View	Visual Mode	The steps of the task are displayed in Visual Mode which displays a plain English text description of each step. More on editing task steps	---
	AML Mode	The steps of the task are displayed in AML (Automate Desktop Markup Language) mode, the internal language used by Automate Desktop. More on editing task steps	---
Insert	Add Variable	Adds a variable to the highlighted section of the Steps pane. More on Variables	CTRL + ALT + V
	Add Comment	Adds a comment to the highlighted section of the Steps pane. More on Comments	CTRL + ALT + C
	Add Attachment	Adds an attachment to the highlighted section of the Steps pane. More on Attachments	---
	Add Label	Adds a label to the highlighted section of the Steps pane. More on Labels	---
Recorder	New Recording	Opens the Automate Desktop**Recorder** – a powerful feature that simplifies the process of automating and recording user interface interactions and actions in Automate Desktop. By using the Recorder's intuitive interface, you can quickly and easily create and add recordings to new or existing tasks. More on the Recorder	CTRL + ALT + R
	Edit	Edits an existing Recorder recording. More on the Recorder	CTRL+ ALT + E
	Split	Splits a Recorder recording into two recordings at the specified step. More on the Recorder	CTRL + ALT + T

Actions Tab Commands

The following table details each command found in the ribbon's **Available Actions** tab along with their associated controls and keyboard hot-key combinations (if applicable). Each command is categorized by the group they reside in.

Group	Command	Description
Actions Panel	Add Step	Gets the action selected from the Available Actions pane and places it as the last step on the Steps pane. More on Steps
	Insert Step	Gets the action selected from the Available Actions pane and places it in the specified location on the Steps pane. More on Steps
	Expand All	Expands all folders in the Available Actions pane. More on Available actions Pane
	Collapse All	Collapses all folders in the Available Actions pane. More on Available Actions Pane
	Categories	Enables/Disables categorized folders in the Available Actions Toolkit (Enabled by default). More on Available actions Pane
	Sort A to Z	Changes the sort order of the current Available Actions view to alphabetical A to Z. Click again to reverse the sort order. More on Available Actions Pane

Group	Command	Description
My Actions Panel	Clear Favorites	Clears the My Actions favorite actions list. More on My Actions pane
	Clear Recent	Clears the My Actions recent list of actions. More on My Actions pane
	Clear All	Clears all the My Actions Favorites, Snippets, Recent, and Frequent lists. More on My Actions pane
	Clear Snippets	Clears the My Actions snippet action list. More on My Actions pane
	Clear Frequent	Clears the My Actions frequent actions list. More on My Actions pane
	Clear Folder	Clears the selected snippet folder in the My Actions pane. More on My Actions pane
	Add to Favorites	Adds the selected action to the Favorites list. More on My Actions pane
	Add as Snippet	Adds the selected step as a snippet. More on My Actions pane
	Create Folder	Creates a snippets folder. More on My Actions pane
	Remove Selected	Removes the selected step, snippet, or region. More on My Actions pane

File Menu

The **File** tab is located in the upper-left corner of the ribbon and presents a menu of commands and operations that do not directly relate to the editing of the task at hand. They include items that normally reside in the **File**menu of legacy systems, such as **New**, **Open**, **Save**, **Print**, and **Close**. The right-hand portion of the menu lists the most recently opened tasks. These are always conveniently visible so that you don't have to search your computer for a task you previously opened or frequently work on. The bottom right corner of the menu contains the **Options**button. Clicking this button opens a **Preferences**dialog that supplies an assortment options used to configure visual and behavioral attributes of the Task Builder.

File Menu Commands

The following table provides a description for each command found when clicking the **Application** button along with their associated controls and keyboard hot-keys (if applicable).

Command	Description	Hot-Key
Help	Opens the embedded help files.	---
New	Creates a new task. Selecting this option adds a new tab in the Steps pane. **NOTE:** Using this option creates an unmanaged task.	CTRL + N
Open...	Opens an existing task. A standard Windows Explorer dialog appears allowing you to navigate to the task (.AML) file to open.	CTRL + O
Save	Saves the current task. If the task being saved is a managed task, it will be saved to its present location. If saving an unmanaged task (for example, created using the **New**option), a standard Windows Explorer dialog appears allowing you to select the folder in which to save the task (.AML) file.	CTRL + S
Save As	Saves a copy of the task file or saves the task file in another format. A standard Windows Explorer dialog appears allowing you to navigate to the location in which to save the task (.AML) file.	SHIFT + CTRL + S
Save All	Save all open tasks.	---
Close	Closes the current task file. If changes were made, a dialog will appear prompting whether to save the changes. Click **Yes** to proceed.	---
Close All	Closes all currently opened tasks. If changes were made to one or more tasks, a dialog will appear prompting whether to save the changes. Click **Yes**to proceed.	---
Print	Prints the steps of the current task as they appear in the Steps pane.	---
Send	Emails the current task to the specified recipient. The available send options are: • **Mail Recipient** - Sends the displayed task in the body of an email. • **Mail Recipient (As Attachment) -** Sends the displayed task as an email attachment. • **Mail All to Recipient (As Attachment) -**Sends all open tasks as email attachments.	---

Command	Description	Hot-Key
Close	Closes the current task file. If changes were made, a dialog will appear prompting whether to save the changes. Click **Yes** to proceed.	---
Close All	Closes all currently opened tasks. If changes were made to one or more tasks, a dialog will appear prompting whether to save the changes. Click **Yes**to proceed.	---
Options	Allows access to available Task Builder Options. The table below lists available options.	---
Exit	Closes the Task Builder.	---

Title Bar

The title bar spans across the top of Task Builder. It contains the title of the current task as well as controls that enable you to set the Task Builder interface to full screen or minimize/maximize the current display. By default, it also contains the Quick Access Toolbar which provides easy one-click access to commonly used controls.

Quick Access Toolbar

The Quick Access toolbar is a small, customizable area to the upper left of the ribbon that provides you with one-click shortcuts to commonly used commands that are independent of the ribbon tabs that are currently displayed. You can add specific commands to the Quick Access Toolbar so they are available no matter which tab you are on. Additionally, you can move the toolbar from one of two possible locations; above or below the ribbon, or you can hide it altogether to save space.

Quick Access Toolbar Default Commands

By default, the Quick Access toolbar exposes single-click buttons that represent the most often used commands, such as **Open**, **Save**, **Undo,Redo**, and **Run.**The following table provides a description of those commands:

Command	Description	Hot-Key
Open	Opens an existing task. A standard Windows Explorer dialog appears allowing you to navigate to the task (.AML) file to open.	CTRL + O
Save	Saves the current task. If the task being saved is a managed task, it will be saved to its present location. If saving an unmanaged task (for example, created using the **New** option), a standard Windows Explorer dialog appears allowing you to select the folder in which to save the task (.AML) file.	CTRL + S
Find	Finds a specific word or phrase. Sub-commands are as follows: • **Find Next** - Finds the next instance of a word or phrase. • **Find Previous** - Finds the previous instance of a word or phrase.	---
Run	Runs the steps of the current task sequentially. Sub-commands are as follows: • **Run All** - Runs all the steps of the current task sequentially. • **Run Selected**- Runs the selected steps. • **Run From Here**- Runs the task from the selected step. • **Step**- Runs the task step by step.	F5

Command	Description	Hot-Key
Undo	Returns to a previous state by undoing the effects of one or more commands. Helpful for undoing mistakes.	CTRL + Z
Redo	Returns back to the state that was previously undone.	CTRL + Y

To add a command to the Quick Access toolbar

1. On the ribbon, click the appropriate tab or group to display the command that you want to add to the Quick Access Toolbar.
2. Right-click the command, and then click **Add to Quick Access Toolbar** on the shortcut menu.

To remove a command from the Quick Access toolbar

1. Right-click the command you want to remove from the Quick Access Toolbar.
2. Click **Remove from Quick Access Toolbar** on the menu that appears.

To remove a default command from the Quick Access toolbar

1. Click the **More Buttons** icon (to the right of the toolbar).
2. On the drop-down menu that appears, select the commands you want to omit from the toolbar. The check mark beside that command will disappear indicating that the command has been removed.
3. To reinstate the command, follow the above directions and simply select the command previously omitted.

To display the Quick Access toolbar below the ribbon

1. Click the **More Buttons** icon (to the right of the toolbar).
2. From the drop-down menu, select the option **Show Quick Access Toolbar Below the Ribbon**. The toolbar is then displayed below the ribbon.
3. To reinstate the toolbar above the ribbon, select the option **Show Quick Access Toolbar Above the Ribbon.**

Access Keys

If you prefer to use the keyboard instead of the mouse, the ribbon provides keyboard shortcuts called Access Keys that enable you to quickly perform operations without reaching for the mouse. Access keys provide a quick and convenient way to use a command by pressing a few keystrokes, no matter where you are in the program.

To use the access keys

1. Press and release the ALT key. The KeyTips are displayed over each feature that is available in the current view.
2. Press the letter, number or character combination shown in the KeyTip over the feature that you want to use. Depending on which letter/number you press, you may be shown additional KeyTips.
3. Continue pressing letters/numbers until you reach the command or option that you want to use.

Other Keyboard Navigation Options

Another way to use the keyboard to work with the ribbon is to move the focus among the tabs and commands until you find the feature that you want to use. The following table lists some ways to move the keyboard focus without using the mouse:

To Do This...	
Select the active tab of the ribbon and activate the access keys.	ALT or F10. Press either of these keys again to move back to the document and cancel the access keys.
Move to another tab of the ribbon.	ALT or F10 to select the active tab, and then LEFT ARROW or RIGHT ARROW
Minimize or restore the ribbon.	CTRL + F1
Move the focus to each command in the ribbon, forward or backward.	ALT or F10, and then TAB or SHIFT + TAB
Move down, up, left, or right among the items in the ribbon.	DOWN ARROW, UP ARROW, LEFT ARROW, or RIGHT ARROW
Activate the selected command or control in the ribbon.	SPACE BAR or ENTER
Open the selected menu or gallery in the ribbon.	SPACE BAR or ENTER

Task Builder Status Bar

The area at the bottom of the Task Builder comprises an intuitive status bar that displays real-time progress of a running task through graphics and text. When a task is run from the Task Builder, the status bar graphically indicates execution state by means of a progress indicator and activity icons. Textual information such as execution status and runtime details are also displayed. The status bar is a great way to provide useful and relevant information without interrupting execution or breaking task flow, which can be very helpful and convenient for task developers, typically during testing periods.

Status Bar Controls

The status bar is divided into sections, each of which displays particular information about the running task. The various elements are detailed below:

Control	Description
Running step/Total steps	Displays the current step being executed as well as the total number of steps the task contains.
Execution status	Displays the status of the currently running task. For example: • **Running** - Task is currently in a running state. • **Completed** - Task completed. • **Error** - Task generated an error.
Progress Bar	Displays total progress of the current step being executed.
Running step action icon	Displays the activity icon associated with the step currently running.
Step execution details	Displays information about the activity that's currently running. This section updates step by step information about the task during execution.

Control	Description
Zoom slider	The zoom slider allows you to increase or decrease the size of objects that appear in the Steps panel. The zoom value is displayed by percentage smaller/bigger than original size. This feature can be used in the following ways: • Move the slider left or right until the desired size is reached. • Click **+**or **-** to zoom in or out in increments. • Right-click the displayed percentage value and select from a drop-down list of predefined values. **NOTE:** To revert back to the default percentage value (100%), left-click the current value that appears.
Zoom level	The zoom level percentage. To revert back to the default percentage value (100%), left-click the current value that appears here.

Task Builder Steps Panel

The Task Builder's Steps panel displays the actions/activitiesthat are selected from the Actions panel that will be carried out when the task executes. During task construction, actions and activities are dragged from the Actions panel onto the Steps panel. During this process, a dialog displaying the properties of the selected action/activity opens and specific parameters and requirements can be viewed or modified. Once parameters are set, the action/activity and its properties are then displayed in the Steps panel and the action becomes a task "step". These steps run automatically in a sequential order when the task is triggered by some event or condition or when started manually by the user.

A single instance of the Task Builder can open multiple tasks, each separated by tabs located at the bottom of the Steps pane. Each tab is labeled with the name of the corresponding task. The steps of the desired task can be viewed by simply selecting the proper tab. When a task is selected, the Steps pane becomes populated with steps of that task and the Status Bar and Debug Pane show data for that task.

Task Builder's Steps panel can be configured to use a predefined color scheme or you can fully customize the collection of colors used to represent the steps of your task and save it as your own personal color scheme.

By default, a task step is comprised of the following:

- Step number
- Unique icon associated with the action
- Visual or AML description of the step (depending on which view is selected from the Ribbon's **View**command group).

Alternatively, step numbers can be omitted, icon sizes can be modified or step descriptions can be fully customized.

> **NOTE:** If you import a task that includes an unlicensed action/activity, the Steps panel will display the unlicensed step (in **Visual**view) as currently unlicensed. Running a task with an unlicensed step will always fail at that step. You can bypass the step by disabling it or removing it altogether.

Task Functions/Variables Panel

In order to make the creation and maintainability of tasks easier and safer, Automate Desktop now supports variable scoping, variable accessibility as well as external tasks and function declarations and execution. The top portion of the Steps pane contains the Task Functions & Task VariablesPanel.

This drop-down panel is used to create Task Functions and Variables and display their properties in a clear and concise manner so the user understands the steps being displayed at any given time are associated with the function/variable being modified.

Context Menu

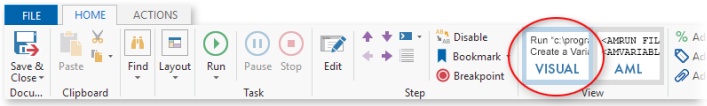
Right-clicking one or more lines of code on the Steps pane opens a pop-up menu that displays a list of available options you can perform for those steps. The table below contains a list of available Steps pane right-click menu items.

Menu Item	Description	Hot-Key
Cut	Cuts the selected steps. To select multiple steps, hold down CTRL during selection. To select all steps, press CTRL+A or click theSelect Allbutton from theFindcommand group of the Ribbon'sHometab.	CTRL + X
Copy	Copies the selected steps to the clipboard. To select multiple steps, hold down CTRL during selection. To select all steps, press CTRL+A or click theSelect Allbutton from theFindcommand group of the Ribbon'sHometab. Copied steps can be pasted in the Steps pane of the current task, another task or an application such as Notepad.	CTRL + C
Copy Description	Copies the description of the as they appear in Visual view	---
Paste	Pastes the previously copied or cut steps. Items are pasted directly below the currently highlighted line in the Steps panel.	CTRL + V
Delete	Deletes the selected steps. To select multiple steps, hold down CTRL during selection.	DEL
Select All	Selects all steps contained in the Steps panel.	CTRL + A
Select Step Number	Opens a *Select Step Number* dialog prompting you to enter the step number to select.	CTRL + G
Select Label	Opens a *Go to Label* dialog prompting you to enter the label to go to.	CTRL + L
Enable	Disables/enables the selected steps. A disabled step will not execute at runtime.	---
Edit Step	Edits the selected or highlighted step. Only a single step can be edited at a time.	---

Menu Item	Description	Hot-Key
Clear Regions	Clears the selected or highlighted regions.	---
Clear All Regions	Clears all regions contained in the current task. Note that this will clear all existing regions whether or not they are selected or highlighted.	---
Move Steps Up	Moves the selected steps one line up.	---
Move Steps Down	Moves the selected steps one line down.	---
Increase Indent	Increases indentation of the selected steps.	CTRL+ RIGHT
Decrease Indent	Decreases indentation of the selected steps.	CTRL+ LEFT
Add to Watch List	Adds the step to the Watch List. You can view watch list items by way of the Watchesdebug pane.	---
Add to Favorites	Adds the selected action to your Favorites list. Favorites as well as most often used and recently used actions can be viewed from the My Actions panel.	---

Custom Step Description

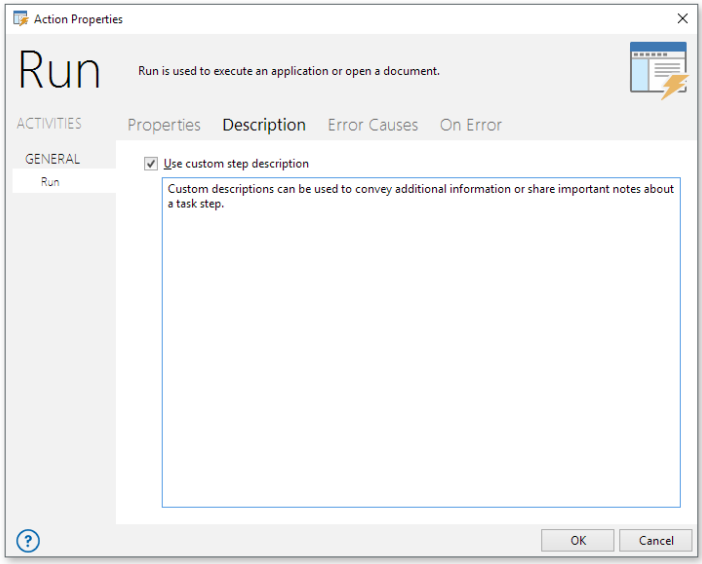
Typically, when a user finishes editing the parameters of an activity, a general description of that activity is displayed in Task Builder's Steps panel, assuming the **View** parameter is currently set to **Visual** mode (circled below). If needed, the default description can be modified or fully replaced with a custom description by way of the **Description** tab properties. This feature can be used to convey additional information about the activity or display special notes or instructions.



> **NOTE:** Custom step description is only supported if the Steps panel view is set to **Visual**mode, which displays the steps in plain English, and not AMLmode, which displays the steps in AML (Automate Markup Language) format.

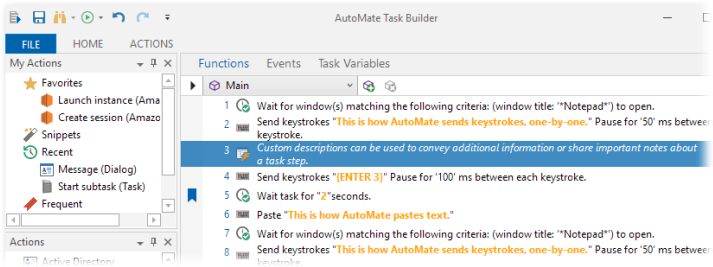
To enter a custom description

1. Open the properties of the activity/step, and then select the **Description** tab.
2. Enable the **Use custom step description** parameter.
3. Enter a desired description in the provided field (as illustrated below), and then select **OK**.



4. The Steps panel displays the custom description entered in place of the

original description (as highlighted below).



NOTE:
Another way to document instructions, notes or other important information directly onto the Steps panel is by adding Comments. If you import a task that includes an unlicensed action / activity, whether or not it contains a custom description, the Steps panel will always display the unlicensed step (in **Visual**view) as currently unlicensed. Running a task with an unlicensed step will always fail at that step. You can bypass the step by disabling it or removing it altogether.

Percent Signs in Advanced Workflows

A percent sign is used as a special character to indicate the beginning and end of an expression. This allows variables, constants and other expressions to be entered in any parameter of a task's properties that accepts expressions. For example: %1+1% inside a task will resolve to 2 at runtime. Below are some common scenarios which involve the use percent signs.

Sending Literal Percent Sign

To send a literal percent sign, escape the percent character. Doubling the percent sign is known as "escaping" the percent sign. For example, to send the literal text 5%, specify 5%%. At runtime the double percentage signs will be recognized and converted into one.

All percent signs are recognized and evaluated by Advanced Workflows that are contained in any parameter that accepts expressions. For example, if an 'Open Webpage' action contained the URL:

https://m

During runtime, Advanced Workflows will detect the percent signs contained in the URL (%admin%) and automatically classify admin as an expression, which eventually fails the task with the error "A variable in the expression does not exist or is misspelled". In such cases, doubling the percent signs will resolve the issue as shown below:

https://

Concatenating Two Values in an Expression

In some cases, it is necessary to concatenate two variables, functions, or some combination thereof. In this case it is critical to remember that two percent signs always mean a literal percent. So the following will NOT work:

%variable1%%variable2%

(INCORRECT)

At runtime, Advanced Workflows would actually see the expression as variable1%variable2 which would result in a Syntax Error. The proper way to combine two values in an expression is to use the ampersand (&) character as follows:

%variable1 & variable2%

(CORRECT)

Common Misconception

A common misconception is that percentage signs are required anytime a variable is used. This is not always the case because percentages surround expressions which may or may not contain variables. For example, in situations where Advanced Workflows requires a variable name (e.g., in the 'Set Variable' action), only the variable name is required. It is permissible, however, to use an expression to specify the variable name so the resolved variable is used.

For example, assume we created a named Var1 with an initial value of Scott. If we wanted to change the value of this variable from Scott to Muscle, we would use a Set Variable action with the properties shown below.

If we add another variable named Var2 and set its initial value to Var1, we could set the Var1 variable to Muscle as we did above by using the expression shown below.

This is because at runtime the %Var2% expression will be evaluated to Var1 before the Set Variable action is executed. The code that executes this example is below.

<AMVARIABLE NAME=Var1Scott/

<AMVARIABLE NAME=Var2Var1/

<AMSET

> **NOTE:** The code can be copied and pasted directly into the Steps pane of the Task Builder.

Testing Tasks Using Run Options

Task execution may happen so rapidly that it is difficult for a user to determine the exact cause of a problematic step. In such cases, the Task Builder encompasses various **Run**options (displayed below) to handle this issue. The **Run Selected** control runs only the selected steps, which is a useful way to ignore execution of steps that are non-problematic. The **Run From Here** control runs the task from the selected step onward. The **Step** control suspends task execution on a step by step basis, allowing you to examine what the task is doing during execution of each step. This is ideal for troubleshooting problematic purposes because it lets you suspend execution at each step as well as view runtime information populated within the various Debug panel views.

> **NOTE:** When suspended, the task is still running but paused between actions. Automate Desktop variablesor datasets retain their values, and the Task Builder's Output panel displays information about the step that is currently running.

Run Controls

The following table describes the Task Builder's list of available Run controls along with their associated icon and equivalent hot-key.

Icon	Name	Description	Hot-key
	Run/Run All	Runs the entire task, from beginning to end, or until an error is encountered, a breakpoint is reached, or the **Pause** button is manually clicked. If the task is manually paused or a breakpointis encountered, execution is suspended indefinitely at the point of the pause or breakpoint. Use other available run options described below to continue execution.	F5
	Run Selected	Runs only the selected (highlighted) steps sequentially, from the lowest to the highest step. To select multiple steps, hold down CTRL during selection.	CTRL + F5
	Run from Here	Runs the task from the selected (highlighted) step until its completion, or until an error is encountered, a breakpoint is reached, or the **Pause** button is manually clicked.	SHIFT + CTRL + F5

Icon	Name	Description	Hot-key
	Step	Runs the task step by step, pausing after each step to allow enough time to examine the information displayed in the Debug panel. To continue to the next step, click **Step** or press **F9**. To run the remaining steps at normal speed, click **Continue** or **Run from Here**. **NOTE:** • Stepping can also be used to step through a task from a breakpoint or paused step. • When execution is paused, task state is suspended, however, functions, variables, and other debugging elements remain in memory. In order to fully stop task execution and reset debugging elements, click **Stop** or press **CTRL+F2**.	F9
	Continue	Continues execution of a paused task from the point of suspension until its completion, or until an error is encountered, a breakpoint is reached, or the **Pause** button is manually clicked.	F5
	Pause	Immediately and indefinitely suspends task execution at a particular step. Click **Continue** to resume execution or click **Step** to run remaining steps one by one.	F6
	Stop	Immediately stops the running task and resets all debugging elements.	CTRL + F2

Run Instructions

To run the entire task

Click the **Run All** button or press F5. This will run all of the steps of the task sequentially from beginning to end (or until an error is encountered, a pause is manually applied, or a breakpoint is reached).

To run one or more selected steps

1. Select the steps you wish to run from the Steps panel. To select more than one step, hold down CTRL during selection.

2. Click **Run Selected** or press CTRL+F5. This will run the specified steps in sequence from the lowest to highest numbered step.

To run the task from a specific step

1. Select the step that should start the execution process.
2. Click **Run From Here** or press SHIFT+CTRL+F5. The steps will run sequentially starting from the step you selected.

To step through a task

1. Click the **Step**button. The first (or selected) step of the task runs. At this time you can:
    a. Examine the contents of your variables by looking at the Variable View of the Debug Window.
    b. Examine the states of any watches you have set, using the Watches View of the Debug Window (see below for more information on watches).
    c. Observe what the previous step may (or may not) have done by reading the contents of the Output View.
2. Continue clicking **Step**to execute the next line until you reach the end of the task or until you have determined the issue.
3. You can also run the rest of the task at regular speed from this point forward by clicking **Run from here**or pressing CTRL+SHIFT +F5. Click **Stop** or press CTRL+F2 at any time to stop a step process.

> **NOTE:** If you import a task that includes an unlicensed action/activity, the Steps panel will display the unlicensed step (in **Visual**view) as currently unlicensed. Running a task that includes an unlicensed step will always fail at that step. You can bypass the step by disabling it or removing it altogether.

More on "Stepping"

“Stepping” is the process of executing a task one step at a time. When clicking the **Run** button, task execution may happen so quickly that it’s too complicated to determine what is causing the problem and where that problem takes place. The **Step** button is ideal for such a situation because clicking this button will execute one step, then wait, providing a chance for the developer to examine what the previous step may (or may not) have done or observe the contents generated in the Debug window in order to better diagnose the task. The **Step**button can be accessed by way of the keyboard by hitting the F9 key.

> **NOTE:** Most Task Builder commands and controls contain a corresponding shortcut key (or hot-key). To determine the appropriate shortcut for a control, simply hover the mouse over it.

Control Running Tasks

You can manually pause or stop a currently running task at any time during its execution.

To suspend a running task

- Click **Pause** or press **F6**. Upon doing so, the task delays execution at the current line. Click **Pause**or press **F6** again to resume execution.

To stop a running task

- Click the **Stop**button or press **CTRL + F2**. The task immediately stops at the current line and resets itself.

> **NOTE:** The **Pause** and **Stop** buttons are usually disabled and are active only during task execution.

Task Variables

Task variables - not to be confused with the Variable Action - provide a means of sharing common data within a single function or between more than one function. The parameters of a task variable are similar to that of a task function which comprise a **Name**, **Type**, and **Accessibility**descriptor. In addition, a task variable includes a **Description**parameter as a way to distinguish each variable. Unlike a task function, however, a task variable cannot be marked as **Optional**. Some advantages of task variables are as follows:

- **Preservation of task-centric values** - Data that is common to an entire task or used by one or more functions are candidates for elevation to a task variable. An example could be a variable to indicate whether the task is in “normal” or “error recovery” mode.
- **Can be used as a “named constant”** - In Automate Desktop, a constant is defined at the system level. However, there are situations where a value is meant to be preserved throughout the lifetime of a task, regardless of function or external task, but not dictated by the system configuration. A task variable can accomplish this, optionally with the read-only option set.
- **Allows information-protection and controls access by external tasks** - This can be accomplished by using the Accessibility preference of a task variable. They control which task variables are merged into a parent task or accessible through a task object.

Task variables, functions and events are created and managed through a drop-down UI display that is accessible from the Steps panel of Task Builder .

> **NOTE:** Task Variables are different from Local Variables which are created using the "Variable - Create" action. Task Variables are additional features aimed for advanced users. You can build tasks without the use of Task Variables and may choose to use them at your own pace.

Scope and Accessibility

Scope and Accessibility provide two different capabilities to Automate Desktop and serve two different but complimentary roles necessary to realize the full benefits of task variables. They are primary building blocks that can be used to build a solid foundation for a rich object-oriented approach to tasks.

Scope

Scope limits a task variable's visibility within a task (that is, using a variable from "the inside"). Without proper scoping, it would not be possible to provide some of the best advantages to function-oriented design, including information-protection, modularity, maintainability and recursion. Scoping helps take large, unruly tasks and enforce logical restrictions to their structure to provide greater readability and maintainability. They can help optimize and enhance task execution speed by reducing the amount of variables that are present in the system at a given time. Scoping also helps avoid unintentional and confusing data changes and variables accesses, leading to easier debugging, and cleaner and more reliable tasks.

> **NOTE:** Task variables are scoped outside of task functions, and all task variables are accessible to all task functions in that task.

Accessibility

Accessibility provides the fundamentals of information-protection, encapsulation and interfacing, all of which are essential for an object-oriented approach to a language. The ability to set task variables and functions as public or private gives a task developer greater control over how a task is used by another task. It makes tasks more portable, manageable and documentable by providing outside access only to those parts of the task that are meant to be used, while providing the user full flexibility of functions. Automate Desktop supports two levels of accessibility:

- **Public**- The variable or function is visible and accessible to external tasks.
- **Private**- The variable or function is not visible or accessible to external tasks.

The accessibility of a task variable can be adjusted to suit the information-protection needs of the task as it relates to an external or sub-task. By default, a task variable is public, meaning it is accessible to an external task or external task function. This is accomplished in different ways, depending on how the external task is referenced, but the behavior of the task variable is identical regardless.

Sub-Tasks

Sub-tasks are task files that are executed within another task by using the Task - Start subtask activity. In this situation, the parent task's (that is, the task executing the Start sub-task step) basic functions, extended functions, public task functions, public task variables, and any local variables (unmarked as private), created up to point where the Start sub-task step is encountered, are accessible to the sub-task. All other variables and functions are not accessible to the sub-task. Conversely, because the Start Task activity is a synchronous operation, the sub-task's public functions and public task variables are not accessible from the parent task. This is fully backward compatible with previous versions of Automate Desktop, since in the past there was only one

“function” (what is now called “main”), no task variables, and all (local) variables and extended functions were considered public.

Creating and Defining Task Variables

Task variables are scoped outside of task functions, and all task variables are accessible to all task functions in that task. They are created and presented in a separate panel located on the Steps panel.

To create and define a task variable

1. In the Task Builder's Steps panel, select Task Variables.
2. Click the **Add Task Variable** button. A panel opens where a new task variable can be added and specific parameters can be set.
3. Enter the following parameters:

Property	Type	Description
Name	Text	The unique name of the task variable to create.
Type	Text (options)	The type of task variable to create. The available options are: • **Variable**- The return value will be in the form of a variable. • **Array**- The return value will be in the form of an array. • **Dataset**- The return value will be in the form of a dataset.
Access Type	Text (options)	The task variable's access type. The available options are: • **Public**- The variable is visible and accessible to external tasks. • **Private**- The variable is not visible or accessible to external tasks.
Initial Value	Text	The initial value of the task variable (if any).
Description	Text	An optional description of the task variable.

4. When finished, click **Save Changes**. The newly created task variable along with its properties appears on the list of task variables available for the task.

Editing and Deleting Task Variables

To edit an existing task variable

1. From the task variables panel, select the variable you wish to edit from the list and then click **Edit**.
2. Make the desired modifications then click **OK** when finished.
3. Reflected changes appear in the main panel.

To delete an existing task variable

1. From the task variables panel, select the variable you wish to delete and click the **Remove**button.
2. The task variable is permanently removed from the list of available task variables.

Creating Variables (Advanced Workflow Module)

A variable (also known as a local variable) is a placeholder for varying or changeable data. Variables play an important role in because they enable developers to write flexible tasks. Rather than entering data directly into a task step, a developer can use variables to represent the data. Then, when the task runs, the variables are replaced with real data. This makes it possible for a task to perform actions on values that may or may not be known until runtime. It also allows a single task the ability to hold different sets of data.

Variables are created and/or set in Task Builder during task creation. They are commonly used when a task involves collecting data from a source and then performing some action on it. You use the variable to contain the collected data, and then set up the actions to be performed on the data by referencing the variable. For example you could create a variable in the beginning of a task that will be populated with the user's input in a form or message box. In a subsequent step you could perform calculations on the data the user entered by referencing the variable.

Creating Variables

The Create variable activity generates a local variable which can be used to store dynamic values for utilization in any step of the task or any sub-tasks started with the Start Task action. The developer can enter a value to initially populate the variable during creation or the value field can be left blank. Instead, variables can be set with a value using the Set Variable action, which adds or changes the contents of an already existing variable. Certain available actions that support populating variables can also set or modify a variable's contents, such as the Input Box action. This action displays an input box allowing the user to enter a value which is saved to the variable specified.

Once a variable is created, it becomes available for use in subsequent steps of the task. It will appear on drop-down lists in places where a variable can be entered, and it can be used in expressions by simply placing the name of the variable between percent signs (%). For example, entering %UserInput% tells to populate the expression with the current value of the variable named UserInput.

It is important to note that in order for a variable to be used in a task step, it must initially be created within an earlier step.

Variable Naming Conventions

Variable names must contain only alphanumeric characters, must start with a letter and cannot contain spaces. Variable names are not case-sensitive. When choosing a variable name, it is good practice to select a name that is descriptive of what the variable holds. For example, if a variable holds the size of a shoe, then name it ShoeSize or TheSize. This makes the task more comprehensible. Also, be sure to avoid using BASIC keywords, functions, or instructions. Names such as DATE or TIME would create a conflict. One way to avoid this is to include distinguishing characters in the variable name such as VAR, THE or MY. For example, a date variable could be named MyDate, DateVar or theDate.

Variable names must be unique within a task, but can be repeated from one task to the next. For example, if you create a variable in one task named UserInput, you can create a variable of the same name in another task without any conflict occurring.

Variable naming restrictions

There are limitations to the names that can be given to variables. These limitations derive from the fact that when the expressions between % signs are evaluated as a script, even if they are a simple variable name. Therefore all BASIC Script keywords, functions names, and operators are forbidden as variables names (e.g. while, wait, like, instr, date, time, now, daysinyear, etc).

Also all Windows environment variables such as PATH, DATE, TMP, PROMPT are also reserved and cannot be declared as new variables. They are, however, accessible and readable, whether or not they were declared “as parameters” in an AMVARIABLE statement.

This is quite a lot of common names which are in fact reserved. Nothing warns that they are not allowed, but the error will appear at execution time, with some strange error message that is all but obvious to understand. A wise precaution to avoid any mistake is to initiate all variable names by a specific (group of) character(s), say v_ (underscore) which then allows variables like v_wait, v_do, v_while, v_path without any ambiguity.

Scoping & Accessibility

Local variables created within a task function (e.g., by using Create Variable, Create Array, etc.) are scoped to that function. Local variables, therefore, are not visible and thus cannot be used outside the function in which they are created. If a variable is created within a function with the same name as a task variable, the local variable “hides” the task variable and takes precedence.

Scoping a created variable to the function in which it is created has the following advantages:

- Variables are only created when required - Because functions are distinct units designed for a single purpose, variables created within them are typically only needed to serve that purpose before returning an end result. Scoping the variables to the function keeps these variables localized to where they are needed. Once their purpose is complete, they are discarded.
- Keeps temporary variables where they are needed - Many functions make use of temporary variables, for example when indexing an array, looping, etc. Local variables provide a means to create indexing or temporary variables that are only available within that function without creating a global variable that can be trampled on by other functions. An example of the danger of using a common index variable without local scoping is creating an index variable named i that, in a loop, calls another function which itself uses a variable i as an index. When the second function is finished, the first function will have the wrong value!

Local variables avoid this problem.

- It does not preclude the use of task variables - A function can still set and retrieve the value of a task variable, or assign a task variable the value of a local variable. This improves readability and keeps the number of variables a user needs to remember or debug to a minimum.
- Makes tasks easier to debug - The use of local variables and task variables means there are less variables the user needs to keep in their head at any given time. “The less you have to keep in mind, the smaller the chance that you’ll make an error because you forgot one of the many details you needed to remember.” Additionally, it provides a means to separate variables in a debugger or other visual display.
- Allows recursion - Recursion is impossible without local variables. Recursion relies on local variables to store the state of the function during each call. If a variable is scoped outside the function, each call of that function will overwrite the data of the previous call, thus rendering the recursion useless.

A local variable’s or local array's accessibility is defined by the Variable is private option on the Create Variable or Create Array step. By default, this option is set to OFF and therefore the variable's default accessibility is public. This means that an external task can access a public local variable.

Sub-tasks

Sub-tasks are task files run synchronously at the step level using the Start Task action. Sub-tasks are treated as individual modules that maintain their own scope and accessibility. Sub-tasks can access public variables, functions and extended functions of the parent task, but not vice versa. Functions and variables contained in the sub-task, however, whether private or public, are accessible to functions called within the sub-task while the sub-task is executing, exactly as if the sub-task were running independently. An important point to note regarding this is how events (which are functions that are optionally implemented by a task and called implicitly by the task engine) are scoped; a sub-task’s events are fired during sub-task execution, not the parent’s. This follows the rules of variable and function scoping and accessibility.

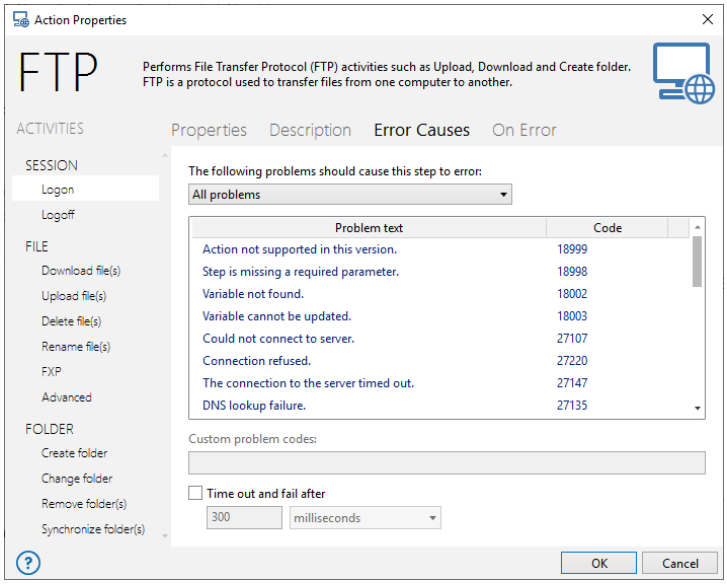
Error Causes

The **Error Causes** properties allows you to modify how this step should behave upon the occurrence of an error. The default behavior is to monitor for the occurrence of all errors, however, these properties can be set in order for this step to ignore certain errors or only react to specific errors. It also allows you to set the length of time this step should be permitted to execute before causing a time out error. If any **Error Causes** conditions are met during task execution, the procedures set under the On Error properties are carried out.

> **NOTE:** All **Error Causes** properties are optional entries.

Practical usage

Particularly used as a way to ignore non-critical errors or overlook anticipated issues in order for task execution to proceed without interruption. Can also be used to set a time out value for time-sensitive steps.



Parameters				
Property	**Type**	**Default**	**Markup**	**Description**
The following problems should cause this step to error	Text	All Problems	`AM_ERRORS=18999,18998,20008`	Allows you to select / deselect specific errors that will cause this step to fail. The available options are: • **All Problems** - Any problem encountered during execution of this step will cause the instructions specified in the **On Error** properties to be carried out. • **Selected Problems** - Only the selected errors will cause the instructions specified in the **On Error** properties to be carried out. Non-selected

Parameters				
Property	**Type**	**Default**	**Markup**	**Description**
				errors are ignored. • **All except Selected** - All non-selected errors will cause the instructions specified in the On Error properties to be carried out. Selected errors are ignored.

Parameters				
Property	**Type**	**Default**	**Markup**	**Description**
Custom problem codes	Text	(Empty)	`AM_ERRORS="18999,18998,20008"`	Allows a custom error code to be entered in case it does not appear in the list of errors. This parameter will adhere to the specifications set under the parameter labeled **The following problems should cause this step to error.** Variables can be used in this parameter. **NOTE:** Use AMError to determine specific information about an error.

Parameters				
Property	**Type**	**Default**	**Markup**	**Description**
Time out and fail after	Number	(Empty)	`AM_TIMEOUT=20`	If enabled, allows you to set the total amount of time this step should be allowed to execute before generating a timeout error. For example, a SQL Query step is set to time out after 30 seconds. If the query took longer than 30 seconds to complete, the step would generate a time out error and the instructions set in the **On Error** properties would be carried out. This parameter is disabled by default.

Parameters				
Property	**Type**	**Default**	**Markup**	**Description**
Timeout scale	Text (options)	Milliseconds	`AM_TIMEOUTSCALE=seconds`	The scale in which the timeout value should be set to. The available options are: • **Milliseconds (default)** - The timeout value is measured in milliseconds. • **Seconds**- The timeout value is measured in seconds. • **Minutes**- The timeout value is measured in minutes. • **Hours**- The timeout value is measured in hours.

On Error

The **Error Causes** properties allows you to modify how this step should behave upon the occurrence of an error. The default behavior is to monitor for the occurrence of all errors, however, these properties can be set in order for this step to ignore certain errors or only react to specific errors. It also allows you to set the length of time this step should be permitted to execute before causing a time out error. If any **Error Causes** conditions are met during task execution, the procedures set under the On Error properties are carried out.

> **NOTE:** All **Error Causes** properties are optional entries.

Practical Usage

Particularly used as a way to ignore non-critical errors or overlook anticipated issues for task execution to proceed without interruption. Can also be used to set a time out value for time-sensitive steps.

Parameters				
Property	**Type**	**Default**	**Markup**	**Description**
The following problems should cause this step to error	Text	All Problems	`AM_ERRORS=18999,18998,20008`	Allows you to select / de-select specific errors that will cause this step to fail.The available options are: • **All Problems** - Any problem encountered during execution of this step will cause the instructions specified in the **On Error** properties to be carried out. • **Selected Problems** - Only the selected errors will cause the instructions specified in the **On Error** properties to be carried out. Non-

Parameters				
Property	**Type**	**Default**	**Markup**	**Description**
				selected errors are ignored. • **All except Selected** - All non-selected errors will cause the instructions specified in the On Error properties to be carried out. Selected errors are ignored.

Parameters				
Property	**Type**	**Default**	**Markup**	**Description**
Custom problem codes	Text	(Empty)	`AM_ERRORS="18999,18998,20008"`	Allows a custom error code to be entered in case it does not appear in the list of errors. This parameter will adhere to the specifications set under the parameter labeled **The following problems should cause this step to error.** Variables can be used in this parameter. **NOTE:** Use AMError to determine specific information about an error.

Parameters				
Property	**Type**	**Default**	**Markup**	**Description**
Time out and fail after	Number	(Empty)	`AM_TIMEOUT=20`	If enabled, allows you to set the total amount of time this step should be allowed to execute before generating a timeout error. For example, a SQL Query step is set to time out after 30 seconds. If the query took longer than 30 seconds to complete, the step would generate a time out error and the instructions set in the **On Error** properties would be carried out. This parameter is disabled by default.

Parameters				
Property	**Type**	**Default**	**Markup**	**Description**
Timeout scale	Text (options)	Milliseconds	`AM_TIMEOUTSCALE=seconds`	The scale in which the timeout value should be set to. The available options are: • **Milliseconds (default)** - The timeout value is measured in milliseconds. • **Seconds**- The timeout value is measured in seconds. • **Minutes**- The timeout value is measured in minutes. • **Hours**- The timeout value is measured in hours.

Error Handling

The Task Builder's three-tiered approach to error handling provides a variety of methods in which to troubleshoot problematic tasks as well as supply alternative techniques to allow a task to recover gracefully from unexpected errors. Error handling can be set by way of the step, task and system level. The flow of error handling takes precedence from step to task to system. For instance, if an error occurs during task execution, the Task Builder first adheres to any exception handling parameters set for the step that caused the error (if any), followed by error handling set for the task level, and conclusively, any system wide error handling parameters.

> **NOTE:** In the Automate Desktop that is bundled in EFT, the Managed Tasks in the Task Administrator are not triggered by EFT event rules. Instead of the Automate Task Administrator, events and triggers are managed by the EFT Event Rules system. (You can copy the managed tasks' AML file (**\ProgramData\Automate\Automate Desktop 2024\Tasks**) and then import or copy it to a task in EFT.)

Step-Level Error Handling

Step-level error handling handles task exceptions on a per step basis. Normally, any failure of a step within a task causes a step error. What causes a step to fail is, however, dependent on the step and it's parameters. These parameters can be adjusted under the **Error Causes**tab of any Task Builder step (as shown below). For additional details, see Error Causes.

If a step fails, the user can select from a number of actions to be carried out. These actions are located in the **On Error** tab of any specific step (as shown below).

Step level error handling takes precedence over task and global lever error handling. When a step level error occurs, a task can alert a user, request user intervention, or with proper exception handling, it can recover on its own.

Task-Level Error Handling

As part of The Task Builder's "tri-level" error handling, errors may be handled on a per task basis. This is ideal if the user wants the Task Builder to perform specific exception handling procedures for a managed task. A task level error occurs when a step within a task fails and Task Builder generates an error.

In most cases, error information is written to a log file so the user can easily track down illusive errors or identify obscure program behavior.

System-Level Error Handling

The Task Builder can handle errors globally for all tasks that run on a system. If any system level error handling parameters are enabled, the Task Builder will act on ALL managed tasks that fail with an error.

Debug Panel Overview

The Debug panel contains nine debug views separated by tabs (the active view's tab is always colored blue). Here, you can select the **Variables**tab to easily view variables and datasets that are contained in the task as well as their initial and current values, or click the **Output** tab to view step by step information about the task during execution. Each debug view supplies a context menu containing relevant options and commands for that particular view.

Debug Panel Views

The available debug tools are listed below:

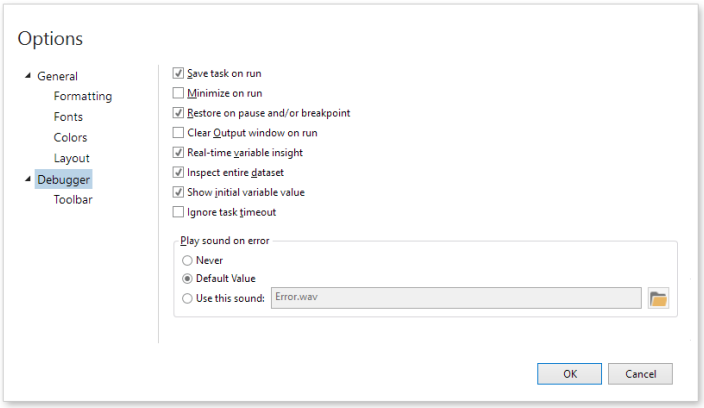
Debug Panel View	Description
Debug Panel - Attachments	Lists all the files that are attached to the current task.
Debug Panel - Breakpoints	Lists all breakpoints contained in the task and their corresponding steps.
Debug Panel - Comments	Displays each comment in the task along with its step number.
Debug Panel - Labels	Lists all labels in the task, including the label name and corresponding step number.
Debug Panel - Output	Shows detailed step by step information about the task during execution.
Debug Panel - Regions	Displays the list of regions contained in the task, including region name and corresponding step number.
Debug Panel - Sessions	Displays a list of steps that contain sessions within the task.
Debug Panel - Stack	Displays the depth of the currently running task. When a sub-task is running, its immediate parent is listed below it.
Debug Panel - Variables	Lists variables and datasets that are contained in the task as well as their initial and current values.
Debug Panel - Watches	Shows all currently set watches and displays the evaluated values for the watched variables and expressions as the task runs.

Task Builder Debugger Options

The Task Builder includes settings that affect its behavior while running a task. In some cases you may want to change these settings to better fit your debugging needs. For instance, you can opt to minimize the Task Builder window during execution to better examine an interactive task, automatically clear the Output Debug Panel after each run, or play a custom sound when an error occurs.

To access Task Builder's Debugger Options page

- Click to **File> Options>Debugger**. Debugger options is a subset of Task Builder Options.



Parameters

The following table describes available Debugger options:

Property	Default	Description
Save task on run	Disabled	If enabled, Task Builder automatically saves changes made to a task when clicking the **Run**button. If the task has not been saved yet, Automate Desktop will prompt the user whether or not to save before running. If disabled, changes will not be saved upon run.
Minimize on run	Disabled	If enabled, Task Builder minimizes to the system tray when execution starts. When the task ends, Task Builder restores itself onto the desktop and highlights the current step or displays **Finished** as the step status in the status bar. If disabled, Task Builder stays on the desktop (does not minimize or hide itself) during task execution. **NOTE:** It is recommended to enable this option when testing tasks that include interactive steps (for example, Send Keystrokes, Move Mouse to Object actions) or steps that interact with other windows (for example, Maximize Window, Minimize Window actions). This is due to leaving the Task Builder window on the desktop may interfere with other windows that appear during runtime. Doing so may result in a Send Keystrokes step, for example, failing to send keystrokes to the proper window or application.
Restore on pause and/or breakpoint	Enabled	If enabled, when task execution is manually paused (when a user clicks the **Pause**button) or pauses at a breakpoint, and the Task Builder window is currently minimized, it restores itself and highlights the current step. When execution continues, the Task Builder window, once again, minimizes to the system tray.
Clear Output window on run	Enabled	If enabled, clears the contents of the Output window before each task execution . If disabled, new debugging output will append existing output accumulated from previous runs.
Limit entries in output panel to	Disabled	If enabled, limits the number of entries in the Output panel to the numeric value entered here. Once the value is exceeded, the oldest entry is deleted. If disabled, entries are not limited.

Property	Default	Description
Real-time variable insight	Enabled	If enabled, the Variables window is updated after each step to show the current value of existing variables on a step by step basis. If disabled, the Variables window is updated only when the task ends or when it is in a paused state (by clicking the **Pause**button, when a Breakpointis encountered or while stepping through with the use of the **Step** button). **WARNING:** Enabling this option could cause Task Builder to run tasks slower.
Inspect entire dataset	Disabled	If enabled, during runtime, extended dataset properties that are normally hidden (for example, creation date/time, total rows) will be displayed in the Variable window. If disabled, only basic dataset properties will be displayed. **WARNING:** Enabling this option could cause Task Builder to run tasks slower.
Show initial variable value	Enabled	If enabled, causes the Variables window to include a column for **Initial Value** in addition to the **Current Value** column. If disabled, only the current value is shown.
Play sound on error	Error.wav	Denotes whether to play a sound when the task stops as a result of an error. The selections are: • **Never** - Do not play a sound when an error occurs. • **Use default sound** - Use the default system error sound, as specified in Window's Control Panel. • **Use this sound** - Specify a valid path and file name of a .wav file to use.

Debugging Tools

Task Builder allows you to visually construct and troubleshoot the steps that an Automate Desktop task performs before it is put into production. It contains many debugging tools that makes it faster and easier to find and resolve issues in your task. You can use breakpoints to pause execution and observe certain elements of a specific step in order to pinpoint the cause of an errant task, or use the various run options to navigate through the steps of your task in different ways, including the ability to start execution from a specific step, run only selected steps, or run each step one by one. The Debug panel allows you to view variable and dataset values or evaluate expressions while the task is suspended.

Debugging Tools and Techniques

The table below describes various Task Builder debugging techniques that you can apply in order to test and troubleshoot a task:

Technique	Description
Attachments	Jumps to a particular step in the Steps panel where a breakpoint resides.
Bookmarks	Removes the selected breakpoints. To select multiple breakpoints, hold down CTRL during selection.
Breakpoints	Removes all breakpoints contained in the task.
Comments	Opens the help topic regarding this subject.
Regions	Jumps to a particular step in the Steps panel where a breakpoint resides.
Run Options	Removes the selected breakpoints. To select multiple breakpoints, hold down CTRL during selection.
Watches	Removes all breakpoints contained in the task.

> **NOTE:** If you import a task that includes an unlicensed action, the Steps panel will display the unlicensed step (in **Visual**view) as currently unlicensed. Running a task that includes an unlicensed step will always fail at that step. You can bypass the step by disabling it or removing it altogether.

Debug Panel - Output

The Output debug panel displays detailed information about a running task and usually provides the best indication of why a task failed. As a task executes, information about each step is logged to the Output panel in real-time, including task step, the action being performed within the step and completion or failure status. If the task fails, extended error information is logged in red for easy detection.

The Output panel is a useful debugging tool because it can contain invaluable information about what a task is doing at any given time. Furthermore, since the data being output is specific to the action being performed, pertinent information unique to each activity's execution may be logged to the Output panel. For example, the File System - Copy activity outputs the name of each file being copied while it is executing. You can determine if the proper files are being copied by simply viewing the Output panel.

Parameters

The Output debug window includes the following fields (columns):

Column header	Description
Step	The step number that the output message refers to.
Function	The function being executed.
Message	A description about the current execution.

Context Menu

Right-clicking inside the Output panel opens a context menu that contains the following items:

Menu item	Description
Auto Scroll	If enabled, causes the Output panel to automatically scroll down to the latest output message that appears during runtime. If disabled, auto scrolling will not be applied.
Copy	Copies the selected (currently highlighted) output data to the clipboard. The contents can then be pasted into any application or window that accepts standard text.
Select All	Selects all data currently displayed in the Output panel.
Clear	Clears all data currently displayed in the Output panel.
Save As...	Saves output data as a (.log) file.
Help	Opens the help topic regarding this debug tool.

Managing Output Data

The contents of the Output panel can be handled in several different ways. New output can be appended to the existing data in the **Output**window, or the window can be cleared before additional data is entered. Output data can be copied to the clipboard, and the contents can then be pasted into any application or window that accepts standard text. You can also save the contents of the **Output**tab to a standard text file.

To copy the contents of the Output panel

1. Right-click anywhere in the **Output**panel, and then select **Copy**.
2. Open the application of your choice (usually a text file) and use the **Paste** function.

To clear the contents of the Output window

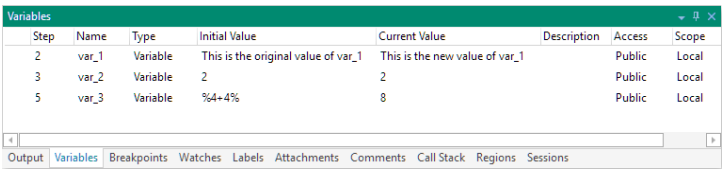
- Right-click anywhere in the **Output** window, and then select **Clear**.

To save output data to a text file

1. Right-click anywhere in the **Output** window, and then select **Save As** .
2. Select a file location (usually a text file).
3. Enter a file name, and then select **Save**.

Debug Panel - Variables

The Variables debug panel is ideal in debugging object types that may contain dynamic data, such as variables, arrays, JSON Objects, and datasets. When a task runs, this panel generates real-time information about such objects including their initial and current value. You can examine content without inserting additional steps to output the values. Similarly, you can insert breakpointsat certain points in your task to halt execution and view this panel to determine if the current values have been properly set or modified.



Parameters

The Variables panel generates information into these columns:

Column header	Description
Inspect	Displays the Inspect icon when a step in the panel is selected. Clicking the icon opens the corresponding dialog, allowing you to further inspect the selected object type.
+/-	When an parent object type has child objects within it, click the expand/collapse icon to expand the parent to view the children. Click the icon again to collapse the parent object type.
Step	The step number in the Steps panel associated to the object type.
Name	The name of the selected object type.
Type	The type of data being displayed, such as a variable, array, JSON Object, dataset, or field (associated to a dataset).
Initial Value	Before the task is run for the first time in a Task Builder session, this column contains the initial value of the variable as set in the variable's/array's properties. If no value was set, this column is blank. An array or dataset can contain multiple rows and columns. During runtime, this section will list the initial value of the rows and columns associated to each array/dataset.

Column header	Description
Current Value	This column reflects the current value of the object type during task execution. **NOTE:** If **Real-Time Variable Insight**is enabled in the Debugger Preferences, the value is updated after each step executes. If **Real-Time Variable Insight**is not enabled, the variable **Current Value** field is updated only when the task is paused, when a breakpoint is encountered or when the task ends.
Description	A description of the variable or array as set in the associated Variable - Create or Array - Create properties dialog. The description does not affect variable/array performance at runtime.
Access	Whether the object type is public or private. Controls how variables are accessed externally.
Scope	Specifies whether the object type's scope is Local or Task: • **Local**- Specifies that the object type is local to the current context or scope. Usually, this means the procedure or function you are currently executing. • **Task**- Specifies that the object type is a task variable which is considered global to the entire task.

Context Menu

Right-click anywhere inside the Variables panel to view the following menu items.

Item	Description
Properties	Opens the properties dialog of the selected object type for viewing or editing purposes.
Inspect	Opens a dialog allowing you to further inspect the selected object type.
Jump to	Jumps to the step number in the Steps panel associated to the object type.
Sort	Sorts the list of object types in the following order: • **Declaration (default**) - Sorts by order of declaration. • **Ascending**- Sorts in ascending alphabetical order. • **Descending**- Sorts in descending alphabetical order.
Copy Name	Copies the name of the object type to the clipboard.

Item	Description
Copy Value	Copies the value of the object type to the clipboard.
Add Variable	Adds a variable to the current task (identical to selecting the Variable - Create activity from the Actions panel).
Add Array	Adds an array to the current task (identical to selecting the Array - Create activity from the Actions panel).
Add Dataset	Adds a dataset tot he current task (identical to selecting the Dataset - Create activity from the Actions panel).
Add to WatchList	Adds the selected object type to the Watches debug panel to examine the state of it while a task is running.
Delete	Deletes the selected object type from the Variables panel.
Delete Locals	Deletes all local object types in the Variables panel.
Delete All	Deletes all objects listed in the Variables panel.
Help	Opens the help topic regarding this debug tool.

Managing Object Types

Object types can be added, edited, or deleted directly from the Variables debug panel. When you edit variables in this way, steps are added, changed, or deleted in the task.

To add a variable, array or dataset object type

1. Right-click anywhere inside the Variables debug panel, and then select **Add Variable**, **Add Array**, or **Add Dataset** from the context menu that appears.
2. Enter the desired properties in the properties dialog, and then click **OK** when finished.

To view/edit an existing object type

1. In the Variables debug panel, double-click on the object type, or right-click on it and select **Properties** from the context menu that appears.
2. View/edit the desired properties in the dialog, and then click **OK**when finished.

To delete an object type

- In the Variables debug panel, right-click on the object type, and then select **Delete**, or select the object type, and then press the **Delete** key on your keyboard.
- To delete only local object types in the Variables debug panel, right-click anywhere inside of it, and then select **Delete Locals**.

- To delete only local object types in the Variables debug panel, right-click anywhere inside of it, and then select **Delete All**.

Debug Panel - Breakpoint

Breakpoints provide a means of pausing execution at a specified step in order for you to inspect certain aspects of the task. In the Steps panel, breakpoints are designated by a red, circled icon located on the left side of the step number. The Breakpoints debug window is used for viewing and managing breakpoints. It lists the step number and textual description of any step that contains a breakpoint. Using this debug window, you can easily jump to any breakpoint step, remove a specific breakpoint or remove all breakpoints. More on Breakpoints

Parameters

The Breakpoints debug screen includes the following fields (columns):

Column header	Description
Step	The step number where the breakpoint resides.
Description	A textual description of the activity where the breakpoint resides. This is identical to the visual step description displayed in the Steps panel.

Context Menu

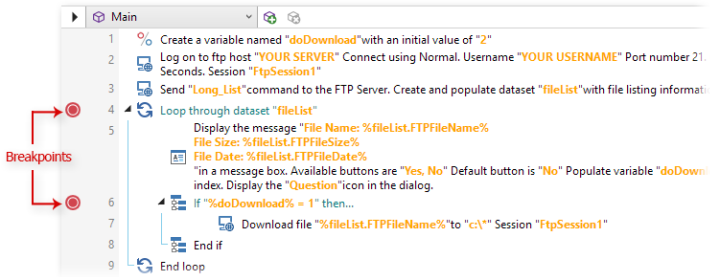
Right-clicking inside the Breakpoints screen opens a context menu with the following items:

Menu Item	Description
Jump To	Jumps to a particular step in the Steps panel where a breakpoint resides.
Remove	Removes the selected breakpoints. To select multiple breakpoints, hold down CTRL during selection.
Remove All	Removes all breakpoints contained in the task.
Help	Opens the help topic regarding this debug tool.

Setting Breakpoints

When a task runs, execution time of each step may only amount to 1 or 2 seconds, making it difficult to examine certain steps that may not be running properly. Breakpoints may be the most ideal solution in this situation. They enable you to suspend task execution where and when you need to. Entering break mode does not stop or end the execution of your task. Elements, such as variables, datasets and functions remain in memory, but their movements and activities are suspended. During the interruption, you can view the Debug panel to acquire knowledge about your task and determine if it is functioning as expected.

Breakpoints can be set at any step and can be used as many times as needed in a single task. They take effect only when a task is run from Task Builder and are ignored when the task is triggered or executed manually outside of Task Builder. Breakpoints are designated by a red, circled icon located on the left side of the step number in the Steps panel. The Breakpoints debug window can be used to examine and manage breakpoints within a given task. Using breakpoints can speed up the debugging process enormously. Without this feature, it would be very difficult to debug a large task.



General Behavior

When a running task reaches a breakpoint step, Task Builder pauses execution, at which point, you can verify proper completion of a particular step or examine the data produced by the assortment of debugging windows located in the Debug panel. This is made possible because a paused task still remains in a running state but suspended between actions. Variables and datasets retain their values and the Output window continues to display detailed information about the task up to the suspended step. You can view step details generated by the Output window or view the Variables window to determine the current value of a certain variable or dataset. In addition, you can manage existing breakpoints or easily jump to a breakpoint step by way of the Breakpoints window.

Depending on what you determine from the data displayed, you can then click **Continue** from the ribbon to continue the task, click **Step**to continue the task step by step, or click **Stop**to halt task execution and reset all debugging elements.

> **NOTE:** Breakpoint symbols are positioned in the same location as bookmark symbols on the Steps panel. If a specific step comprises both, the icon will contain a bookmark symbol overlaying a breakpoint symbol.

To set a single breakpoint, do one of the following

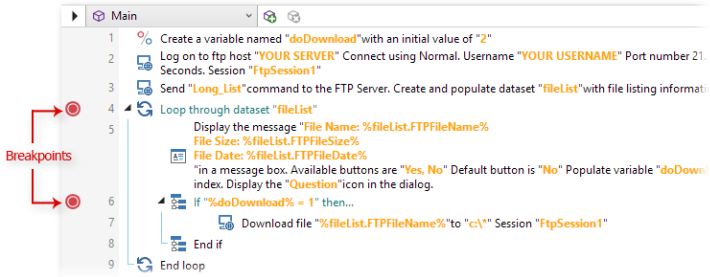
- From within the Steps panel, click the gray margin to the left of the step number on the line where you want to set the breakpoint.
- Select (highlight) the step you want to place a breakpoint and on the **Home**tab of the ribbon, click the **Breakpoint**command from the **Step** command group.

To set multiple breakpoints simultaneously

1. From the Steps panel, select the steps in which to place a breakpoint. To select more than one step, hold down CTRL during selection.
2. From the Ribbon control, go to the **Home** tab and click **Breakpoint** from the **Step** command group.

About Bookmarks

Bookmarks are a means of marking steps in a task with placeholders so you can find them easily during construction or testing. Bookmarks can be set at any step and can be used as many times as needed in a single task. They take effect only when a task is run from Task Builder and are ignored when the task is triggered or executed manually outside of Task Builder. In the Steps panel, bookmarks are indicated by a blue ribbon icon located on the left side of the step number (as shown below). You can mark steps in your task with bookmarks and then navigate directly to those steps by clicking the **Next Bookmark**or **Previous Bookmark** ribbon controls.

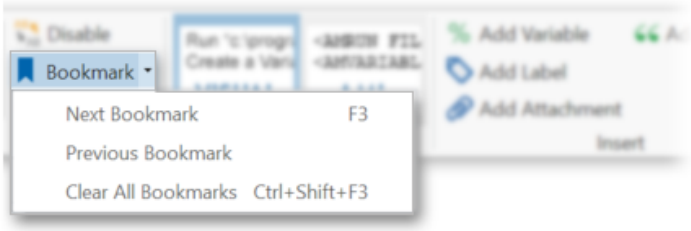


To set a bookmark

1. In the Task Builder's Steps panel, select the steps to bookmark. To select more than one step, hold down CTRL during selection.
2. From the ribbon's **Home**tab, click **Bookmark** from the **Step** command group.

To navigate to a bookmark

1. From the ribbon control's **Home** tab, click the down arrow located on the right side of the **Bookmark**control.
2. Click **Next Bookmark** to jump to the next bookmark or**Previous Bookmark** to jump to the previous bookmark.



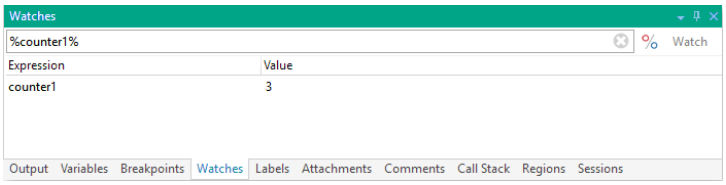
To clear a bookmark

1. In the Task Builder's Steps panel, select the steps that contain the bookmarks you wish to clear. To select more than one step, hold down CTRL during selection.
2. From the ribbon's **Home**tab, click **Bookmark** from the **Step** command group.

> **NOTE:** Bookmark symbols are positioned in the same location as breakpoint symbols on the Steps panel. If a specific step comprises both, the icon will display a bookmark symbol overlaying a breakpoint symbol.

Debug Panel - Watches

The Watches debug panel can store several variables and expressions that you want to view over the course of the debugging session. You can set a watch on a variable used in the task or you can enter an expression to create a more complex watch. You can use the Watches debug view to add, remove, or change watches. After each step executes, any variables and expressions listed are re-evaluated and updated with their current values. Watches go beyond the Variable window by providing an intuitive means of testing variable or task states while a task is executing. More on Watches



Parameters

The Watches window includes the following fields (columns):

Column header	Description
Expression	The syntax of the watch. This can be simply a variable name or a complex expression.
Value	The result of the watch expression. This is updated with each step execution while the task is running.

Context Menu

Right-click inside the Watches window to view the following menu items:

Menu item	Description
Change	Renames the selected variable or modifies the selected expression.
Remove	Removes the selected item. To select multiple items, hold down CTRL during selection.
Remove All	Removes all items listed.
Help	Opens the help topic regarding this debug tool.

Using Watches

A Watch is a debugging feature used for examining the state of variables and other expressions within a running task. A watch can simply be the name of a variable. For example, to watch the value of a variable named `TotalCount`, add a watch that contains simply `%TotalCount%`. Embedded expressions can also be used within a watch, using the same syntax as a standard Automate Desktopembedded expression. For example, to watch the length of an Automate Desktop variable named myName, add a watch `%Len(myName)%`.

The Watches debug panel allows you to add, remove or modify items to watch. It displays the list of added watches and updates their value as the task runs. This way, watches can be re-evaluated after each task step is executed. Watches are mainly used for debugging, therefore, they are ignored when a task is executed as a result of a trigger or executed manually from the Task Administrator.

The Watches debug panel is a place where you can enter variable names and expressions that you want to watch during a debugging session.

To watch a variable

- Enter the variable to watch in one of the following ways:
  - In the Steps panel of the Task Builder, right-click the Create variable step associated with the variable you want to watch and select **Add to WatchList**.
  - In the Variables debug panel of the Task Builder, right-click the variable you want to watch and select **Add to WatchList**.
  - In the Watches debug panel, type the name of the variable in the provided text box and click **Watch**.

To watch an expression

1. In the Watches debug panel, enter the expression to watch in one of the following ways:
   a. Type the expression into the text box. For example, to evaluate the length of an Automate Desktop variable named `myName`, enter `Len(myName)`.
   b. Click the percent icon located to the right of the Watches text box. When the Expression Builder dialog appears, use it to create an expression to watch. Click **Insert**when finished.
2. Click **Watch**.The expression and its current value (if applicable) is added to the **Watches** debug panel.

To modify a watch

1. In the **Watches**debug panel, right-click the desired watch and select **Change**.
2. Enter the new variable or expression name for the watch, and then press **Enter**.

To remove a watch

- Select the watch to be removed, and then press the **Delete** key.
- Right-click on the desired watch, and then select **Remove**.
- To remove all watches, right-click on any watch and select **Remove All**.

> **NOTE:** Using watches can affect runtime performance in the debugger on slower machines. If debugging speed becomes a factor, try removing watches that are no longer needed. This does not apply to runtime performance outside the debugger, as watches are ignored when the task is executed outside Task Builder

Debug Panel - Labels

A Label can be used as a "bookmark" in a task. Labels can be placed at specific steps in a task to mark them as reference points for Goto activities. Labels can be used in step level error handling by setting up a Goto action to be executed if a step error occurs. The Labels debug panel displays labels that are contained in a task, including the name of the label and corresponding step number. This debug tool also allows you to create labels to add to the task. More on Labels

Parameters

The Labels debug screen includes the following fields (columns):

Column header	Description
Step	The step number where the label resides.
Label	The name of the label (this can be a brief description of the label).

Context Menu

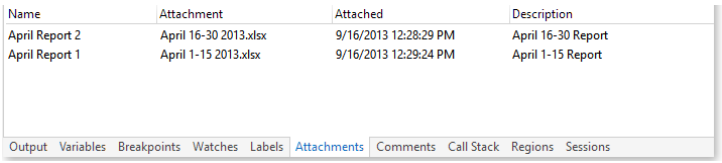
Right-clicking anywhere inside the Labels screen opens a context menu with the following items:

Menu Item	Description
Add	Adds a label to the task. To add a label to a specific step, highlight the step from the Steps panel, then right-click inside the **Labels**tab and select **Add**.
Properties	Opens the properties dialog associated to the label in order to modify its settings. This item is active only when a right-click is performed on a label.
Remove	Removes the selected labels. To select multiple labels, hold down CTRL during selection. This item is active only when a right-click is performed on a label.
Jump To	Jumps to the step in the Steps panel where the specified label is located. This item is active only when a right-click is performed on a label.
Stay On Top	If enabled, after undocking this panel, it will stay on top of all other undocked panels. This option is disabled by default.

Menu Item	Description
Dockable	If enabled, allows the panel to be docked to its base once it is undocked. If disabled, you will not be able to re-dock the panel once it is undocked. This option is enabled by default. You can undock a panel by holding down and dragging its title bar away from the main window or double-clicking the title bar.
Help	Opens the help topic regarding this debug tool.

Debug Panel - Attachments

Attachments are files of any type that are wrapped and accessible from an Automate Desktop task. These files can be easily exported or deployed along with their associated task allowing them to be more transportable and manageable. At runtime, attachments are automatically "unwrapped" to a local directory where they can be accessed by the task. The Attachments debug panel displays any files that are currently attached to the task. It also allows you to add a new attachment to the task as well as modify or remove existing attachments. More on Attachments



Parameters

The Attachments debug screen contains the following column headers:

Column header	Description
Name	The name of the attachment.
Attachment	The file name (including extension) of the attachment.
Attached	The date and time when the file was initially attached to the task.
Description	A user defined description of the attachment (this property is optional, therefore, may appear blank).

Context Menu

Right-clicking anywhere inside the Attachments screen displays a context menu with the following items:

Menu item	Description
Add	Adds a new attachment to the task.
Properties	Opens the **Attachment**dialog to display the properties associated to the selected attachment.
Refresh	Refreshes the Attachments list

Menu item	Description
Remove	Removes the selected attachments. To select more than one attachment, hold down CTRL during selection. **NOTE:** When you remove an attachment, be sure to remove all references to the attachment from the task, otherwise the task may fail to execute properly.
Remove All	Removes all attachments that exist in a task. **NOTE:** When you remove an attachment, be sure to remove all references to the attachment from the task, otherwise the task may fail to execute properly.
Help	Opens the help topic regarding this debug tool.

To attach a file to a task

1. Right-click anywhere inside the Attachments debug panel and select **Add**from the context menu that appears. This opens a dialog titled **Attachment** (shown below).
2. Enter the following information:
    - **Name**- The name of the attachment (this value is what you will use as a placeholder for the file).
    - **Attachment file** - The full path and file name of the attachment file. Use the folder icon to browse to the file you wish to attach.
    - **Description**- An optional description of the attachment.
3. Select **OK**. The new attachment and its properties are displayed in the Attachments Debug panel.

    NOTE: Multiple files of any type and size can be attached to a task, however, be aware that the size of the task file expands with the size and number of attachments, which may affect performance. Multiple or large sized attachments used in a single task may slow down task execution.

To remove one or more existing attachments

1. From the Attachments debug panel, select existing attachments you wish to remove.
    - To select multiple attachments, hold down CTRL during selection.
2. Right-click the attachments and select **Remove**from the context menu.
    - To remove all existing attachments, select **Remove All**.

> **NOTE:** After removing an attachment, make sure to remove all references to it in any step parameter to ensure that no attachment related error occurs during runtime.

To modify an existing attachment

1. From the Attachments debug panel, right-click the attachment you wish to modify and select **Properties**from the context menu. This opens the **Attachment**dialog.
2. Make the desired adjustments.
3. Upon completion, click **OK** to save changes and close the dialog.

> **NOTE:** If modifications to the original attachment name is made, make sure to update any step parameters referencing the original name to reflect the new name to ensure that no attachment related error occurs during runtime.

Adding Attachments

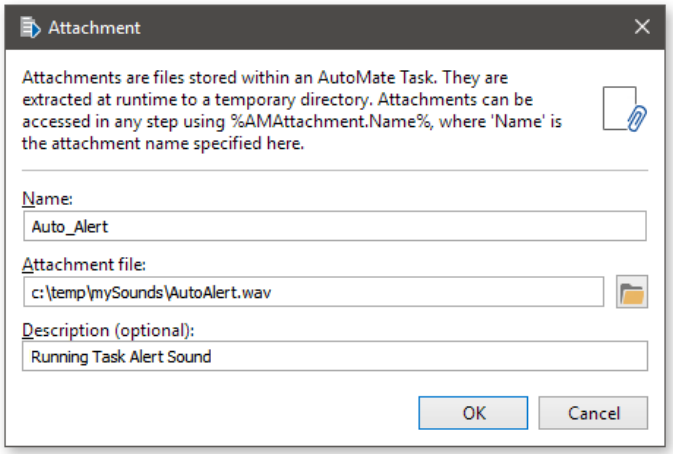
Attachments allow files of any type to be embedded within a task so that third-party elements can be incorporated for greater portability. At runtime, attachments are automatically "unwrapped" to the local temp directory where they can be accessed by the task. For example, you can create a task that plays a unique sound when a particular event occurs by attaching the associated sound (`.wav` or `.mp3`) file to it. When deploying or exporting this task to other Automate Desktop clients, the addition of the sound file as an attachment ensures that it will always be present and accessible on any system.

Attachments are added and managed by way of the Task Builder's Attachments Debug Panel. It displays any files that are currently attached to the task along with their original file name and extension.

To attach a file to a task

1. Do one of the following to open the Attachment Explorer window:
   - Right-click anywhere inside the **Attachments**debug window and select **Add** on the context menu.
   - Click **Add Attachment** on the **Insert** command group of the ribbon.
   - In the Attachment Explorer window, navigate to, and select the file you want to attach, then click **Open**. This attaches the file to the task and the attachment properties (described below) are displayed in the **Attachments** debug window.
2. In the **Attachments** debug window, view or enter the following information:
   - **Name**- The name of the attachment (required). The name you enter will be used as a placeholder for the file during runtime, therefore, the following rules apply when specifying attachment names:
     - Names must contain only alphanumeric characters.
     - Must begin with a letter.
     - Cannot contain any spaces.
   - **Attachment** - The file name of the attachment file. Use the folder icon to browse to the file you wish to attach.
   - **Description**- A user defined description of the attachment (optional).
   - **Attached** - The date and time the file was initially attached to the task (this value is read-only).
3. Upon completion, click **OK**. The new attachment and its properties are displayed in the **Attachments Debug** panel.

> **NOTE:** Multiple files of any type and size can be attached to a task, however, be aware that the size of the task file expands with the size and number of attachments, which may affect performance. Multiple or large-sized attachments used in a single task may slow down task execution.



Accessing Attachments

Once an attachment is added to a task, it can be accessed in any step by entering:

`%AMAttachment.Name%`

Where `[Name]` is the name of the attachment specified in the **Name** parameter of the **Attachment** dialog. For example, assume you created an attachment identical to the one displayed above. In order to play the attachment file `c:\temp\mySounds\AutoAlert.wav` using a Play Audio activity during runtime, simply enter `%AMAttachment.Auto_Alert%` in the **Audio files to play** parameter of this activity.

`AMAttachment.Name` is essentially an Automate Desktop dataset used as a placeholder for the attachment file during runtime. The file itself is unwrapped and saved to the local temp directory. This directory may vary depending on the operating system. On Windows 10, this directory is `C:\Users\[username]\AppData\Local\Temp\attachmentFile.txt`.

Debug Panel - Comments

The Comments debug panel reveals a list of comments included in the task along with the step number in which they are located. You can use this panel to quickly jump to any step that includes a comment. You can also use it to add, modify, or remove one or more comments. More on Comments

Parameters

The Comments window includes the following fields (columns):

Column header	Description
Step	The step number where the comment resides.
Comment	The text description of the comment.

Context Menu

Right-clicking a specific comment or an empty region inside the Comments screen opens a context menu with the following items:

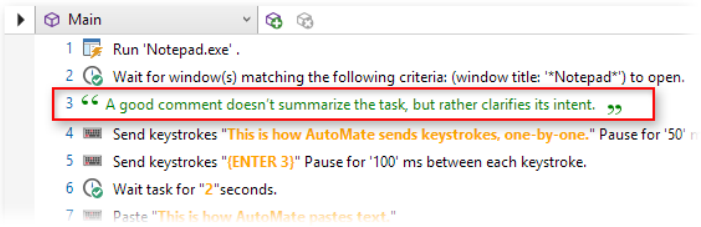
Menu item	Description
Add	Adds a comment to the task. To insert a comment at a specific step, first click the desired step in the Steps panel. The comment is added directly above the selected step. If no step is selected, the comment is inserted at the end (last step) of the task.
Properties	Opens the selected comment's dialog allowing you to view or modify the comment. This item is active only if a comment is selected.
Remove	Removes the selected comments. To select multiple comments, hold down CTRL during selection. This item is active only if a comment is selected.
Jump To	Jumps to the step where the selected comment is located. This item is active only if a comment is selected.
Help	Opens the help topic regarding this debug tool.

Adding Comments

Comments are used to embed user readable annotations in the steps of a task, usually with the purpose of making the task easier to understand. Comments can be used to summarize the task, explain the intent of a specific step, document instructions, enter notes, reminders or other important information. Comments are ignored by Automate Desktop during runtime. For debugging convenience, the Comments Debug Panel displays each comment embedded in a task and their associated step number.

To add a comment

1. From the Ribbon's **Insert**command group, select **Add Comment** or press CTRL+ALT+C. A new Comment step is added in the Task Builder's Steps panel at the end of your task.
2. Click inside the **Enter a comment...** text-box and enter your comment. The new comment is colored green by default, however, you can change the default color by way of Color Options.
3. Use the **Up** or **Down** arrows to move the comment to the desired step or use your mouse to drag and drop the comment to the desired step.



> **NOTE:** Comments can also be added from the Debug panel by clicking the **Comments**tab, right-clicking inside the panel, and then selecting **Add**from the context menu.

Debug Panel - Call Stack

A stack is a dynamic data structure that stores information about the active sub-tasks contained in a task. The Call Stack debug window changes dynamically when sub-tasks are used. It displays execution depth of the current task and allows you to keep track of the point at which each active sub-task should return control to the main task when it finishes executing.

Parameters

The Call Stack debug window generates information into a single column:

Column header	Description
Name	The name of the current task and task function are enclosed inside [] brackets followed by the current step number (for example, `[TheTaskName::Main] Step #10`). **NOTE:** If no task function is selected, the default task function named "Main" will be displayed.

Context Menu

Right-clicking inside the Output panel opens a context menu that contains the following items.

Menu item	Description
Jump to	Jumps to the current step in the Steps panel. **NOTE:** Use a breakpoint to pause the task at a specific step.
Help	Opens the help topic regarding this debug tool.

Debug Panel - Regions

A region is a named section of task steps that can be collapsed as required in order to hide their contents. The use of regions can effectively group a task into sections, thus, can be useful for organizing lengthy tasks and making complex tasks more comprehensible. You can easily expand a region at a click of a button to access steps that you need to work on and collapse the region upon completion. The Regions debug panel lists existing regions within a task, including the name of the region, its starting step and ending step. It also allows you to jump to a particular region, clear a specific region or clear all regions that exist in the task. More on Regions

Parameters

The Regions debug window generates information divided into the following columns:

Column Header	Description
Starting Step	The step where the selected region starts.
Ending Step	The step where the selected region ends.
Region	The name of the selected region.

Context Menu

Right-click anywhere inside the Regions window to view the following properties:

Menu Item	Description
Jump To	Jumps to the step where the selected region is located.
Clear Region	Removes the selected regions. To select multiple regions, hold down CTRL during selection.
Clear All Regions	Removes all existing regions.
Help	Opens the help topic regarding this debug tool.

About Regions

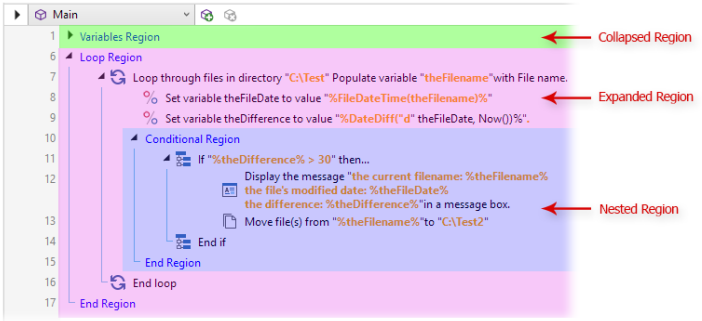
A region is a uniquely named section of a task that can be hidden from view as required. This allows areas of a task to be organized into separate segments, thus, making it less cluttered and more manageable. When a region is collapsed, contents are hidden from view and the region appears as a single step in the task. When a task runs from Task Builder, collapsed regions expand automatically so the developer can view each step as it executes. Upon task completion, regions are re-collapsed to their former state. Automate Desktop supports nested regions (region within a region) to further expand their capabilities.

Regions have no effect on the final, developed task nor does it influence its execution. They only affect the manner in which task steps are visually displayed in Task Builder. Regions can be created to categorize blocks of steps in a task based on common functionality or actions. A unique name can be entered for a region as a way to ascertain its contents when it is collapsed. If a particular step inside a region needs to be viewed or modified, simply expand the region that contains that step while the rest of the regions remain hidden from view.

The Regions debug panel lists existing regions within a task, including the name of the region, its starting step and ending step. It also allows you to jump to a particular region, clear a specific region or clear all regions that exist in the task.

Creating and Populating Regions

You create a region by selecting one or more existing steps and clicking the **Create Region** command on the ribbon or context menu. When a region is created, its default name is always 'New Region.' It is important that you enter a unique name for newly created regions in order to avoid confusion. A collapsed region is designated by a down arrow symbol in the margin near the region. The down arrow symbol can be clicked to expand the region. Once expanded, the down arrow is replaced with an up arrow and a line terminating at the end of the region. The up arrow can be clicked to re-collapse the region. The image below displays an example of a collapsed and expanded region.



To create a region

1. Highlight the steps in the Steps panel you wish to place in a region. To highlight multiple steps, hold down CTRL during selection (selected steps must be sequential).
2. Do one of the following:
    a. Click the **Create Region** button located on the ribbon's **Step**command group.
    b. Right-click and select **Region** > **Create Region** from the context menu that appears.
    c. Press CTRL + R on your keyboard.

A new region is added to the Steps panel populated with the steps you initially selected with the default name supplied for the region highlighted. Simply type over the default name of the region to give it a unique name.

To add a new action or activity to an existing region

1. Expand the region you wish to add an action to by double-clicking the region name or clicking the expand symbol to the left of the region name.
2. Drag the desired action or activity from the Actions panel onto the desired area of the region. A blue line appears in the Steps panel signifying the section in which the action or activity will be placed.
3. Release the mouse button when the blue line arrives at the section of the region you wish to drop the action or activity.

To move existing steps onto a region

1. Expand the region you wish to move existing steps to by double-clicking the region name or clicking the expand symbol to the left of the region name.
2. Highlight the steps that are currently outside of the region you wish to include. To highlight multiple steps, hold down CTRL during selection (selected steps must be sequential in order).
3. Drag the steps to the desired part of the region. A blue line will appear signifying the section of the region in which the steps will be placed.
4. Release the mouse button when the blue line arrives at the section of the region you wish to drop the steps.

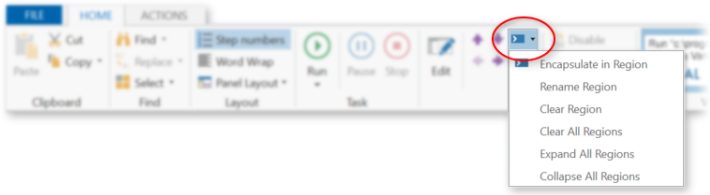
To create a nested region (region within a region)

1. Expand the region you wish to add a sub-region to.
2. Highlight the steps within that region that you would like to place in the sub-region.

3. Click the **Create Region** button from the Task Builder Ribbon's **Step** command group or right-click and select **Create Region**. A new sub-region is added inside the parent region.
4. Click the newly created sub-region to rename it.

Managing Regions

Existing regions can be expanded, collapsed, renamed, modified or cleared. For example, when you are finished constructing your task, you may opt to remove all existing regions with the **Clear All Regions** command. All region related commands are located on the ribbon's **Home** tab in the **Step** command group (circled below) or by way of a context menu that appears when you right-click a region inside the Steps panel.



To expand all regions simultaneously

- Select **Expand All Regions** from the Ribbon's **Step** command group or right-click menu.

To collapse all regions simultaneously

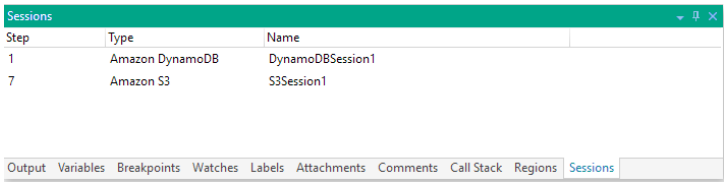
- Select **Collapse All Regions** from the Ribbon's **Step** command group or right-click menu.

To clear one or more regions

1. Right-click the step that contains the region's name and select **Clear Region**.
2. To clear all existing regions, right-click any step that contains a region's title and select **Clear All Regions**.

Debug Panel - Sessions

The Sessions debug panel can be used to display a list of steps that contain sessions within the task.



Parameters

The Sessions debug window includes the following fields (columns):

Column header	Description
Step	The step number where the session resides.
Type	The action that the session derives from.
Name	The name of the session.

Menu Items

Right-click inside the Sessions window to view the following menu items:

Menu item	Description
Jump To	Allows you to jump to the specified session.
Help	Opens the help topic regarding this debug tool.

Advanced Workflow Module Features and Benefits

Advanced Workflows is a powerful tool that allows rapid construction of Windows automation routines via drag and drop without any programming. It replaces legacy batch files, scripts and custom application development, enabling complete IT Process automation without writing a single line of code. Advanced Workflows provides an incredibly easy-to-use, intuitive interface for developing automation applications. The basic building blocks are called actions, which are plain-English, drag-and-drop, fill-in-the-blank tools developers use to build Tasks. Developers simply drag-and-drop actions in Task Builder to build a series of Steps which collectively make up the task.

Available Actions & Activities

Includes 100s of actions and activities that involve extensive support for FTP/SFTP, SQL, Email, HTTP, VB Scripts, VMWare Host and VMWare Guest, Services, Environment Variables, Exchange, MSMQ and many more. This list does not begin to address all the possible automated solutions that can be constructed and deployed. A task can contain any number of actions/activities in any order, creating limitless possibilities.

Intuitive Task Development & Debugging

The Task Builderis an intuitive interface for developing automation applications. It is used to visually construct and examine the steps that a task should carry out when it is run. To ensure that newly created tasks are working properly before they are put into production, the Task Builder also includes a variety of testing and debugging features that outputs real-time information about a running task. They enable monitoring of each step during task execution, allow inspection of variables, datasets and other dynamic data and aid developers with troubleshooting important aspects of a task as it is being constructed.

Variable Support

Includes full support for variables that are used to pass dynamic data during task execution and also supports one and two-dimensional arrays for implementing more complex logic to tasks. Additionally, many actions support the creation of datasets, which can hold multiple rows and columns of dynamic data. This is useful when retrieving data that describes a collection of information such as a database or spreadsheet.

Replaces Code

Reduces costs and hassles associated with developing and maintaining code, scripts, and batch files. For developers, increases the speed of development without sacrificing power, saving time and future code maintenance hassles. For non-developers, provides the simplicity to complex processes without the need for code or syntax.

Ease of Use

Provides an incredibly user-friendly, yet intuitive set of interfaces allowing you to visually create, manage, and execute your automated tasks without requiring any programming expertise. Instead of writing scripts and batch files, business and IT processes are created using the Task Builder interface which contains over 300 prebuilt actions and activities that you can easily drag-and-drop together to form powerful automated tasks.

Saves Time & Reduces Errors

Network managers and IT administrators can eliminate time spent on repetitive IT processes so they can focus on other aspects of their jobs. Additionally, automation eliminates errors introduced during manual processes that often result in network downtime, delayed access to data, and user complaints. Streamline inefficient processes and operations with reliable, repeatable, automation and eliminating errors introduced by process delays and repetitive worker activities.

Accelerates flow of information

Drag-and-drop building enables tasks to be constructed rapidly. This accelerates data flows, allowing business users and decision-makers to become more effective and efficient by delivering real-time access to accurate data.

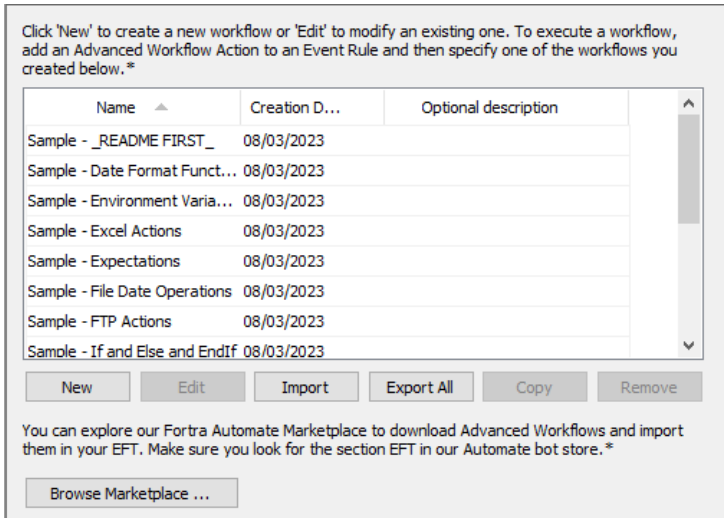
Creating Workflows for Use in an Event Rule

(Requires Advanced Workflow Module) Similar to Commands, Workflows are used in Event Rules as Actions or triggers. When you create a Workflow, it is saved in the SQLite database file in **C:\ProgramData\Globalscape\EFT Server**.

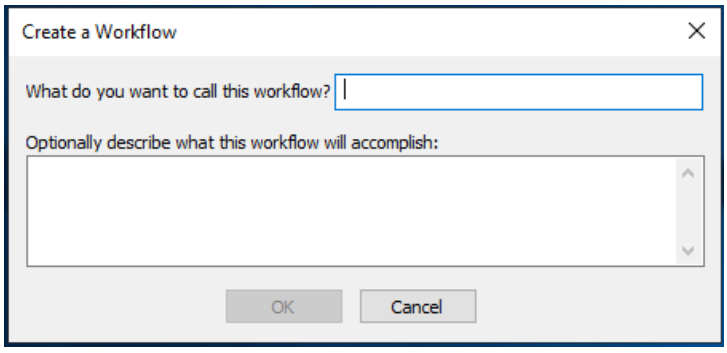
During the Advanced Workflow trial, when a new Workflow is created, a message appears (prior to the **Create a Workflow** dialog box) informing you that the Advanced Workflow module is an optional module and that the trial begins when the first Workflow is created.

To create a Workflow

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Advanced Workflows** node.
3. In the right pane, the **Advanced Workflows** tab appears.

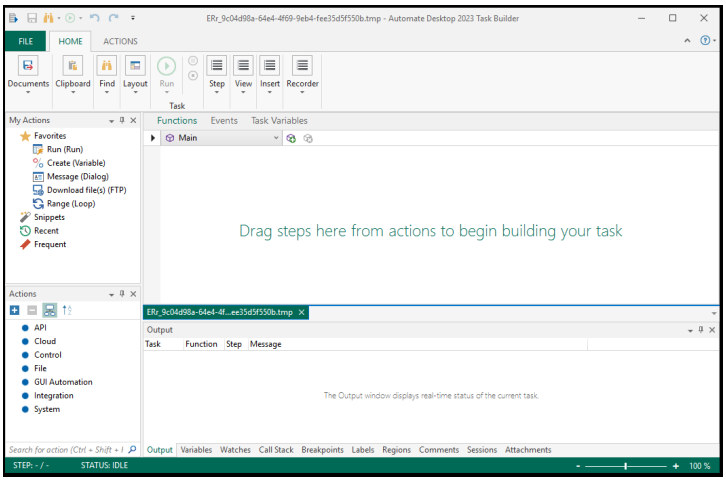


4. In the right pane, click **New**. The **Create a Workflow** dialog box appears.

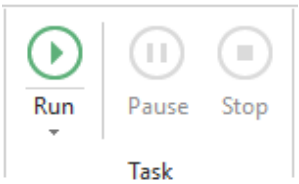


5. In the **What do you want to call this workflow** box, specify a name for the Workflow. When you add the workflow to Event Rules, the name you specify here appears in the Rule.

6. (Optional) Provide a description of the Workflow, and then click **OK**. The Workflow **Task Builder** appears.



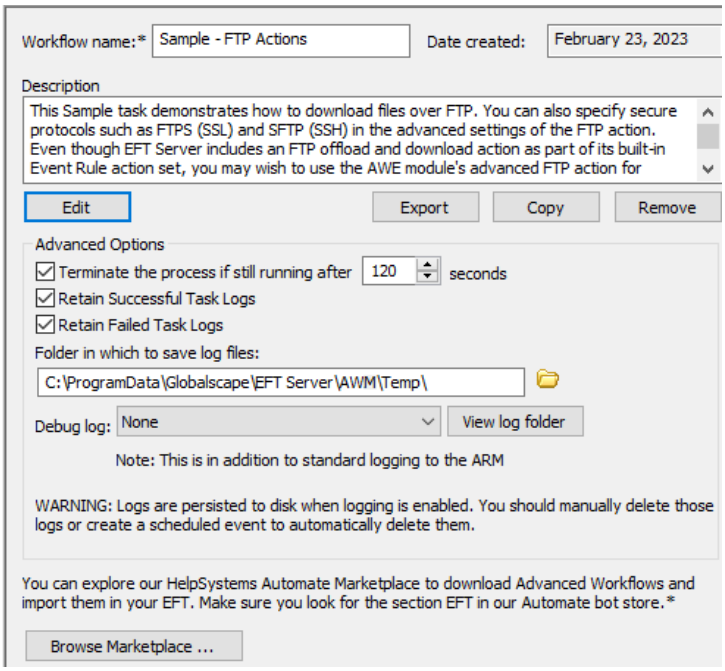
7. The tree in the left pane lists the steps that you can add to the Workflow. The right pane displays the steps in the Workflow.
8. Drag items from the **Actions** list to the **Steps**pane to create your Workflow.
9. Use the **Run**icon on the Debug toolbar to test the steps. You can run the whole Workflow all at once, run only a selected step, or run the whole Workflow starting with a step other than the first step.



The Output pane displays the result of each step. For example:

```
Executing line 5
Starting Input Box with message "What is your name?"...
Creating message box "What is your name?"...  >
Populating variable "theUserName"...
Finished Input Box "What is your name?".
The step was okay.
```

10. After you have created your Workflow, click **Save and Close**. The Workflow appears in the **Advanced Workflows** pane of the Site and is ready to be used in Event Rules.

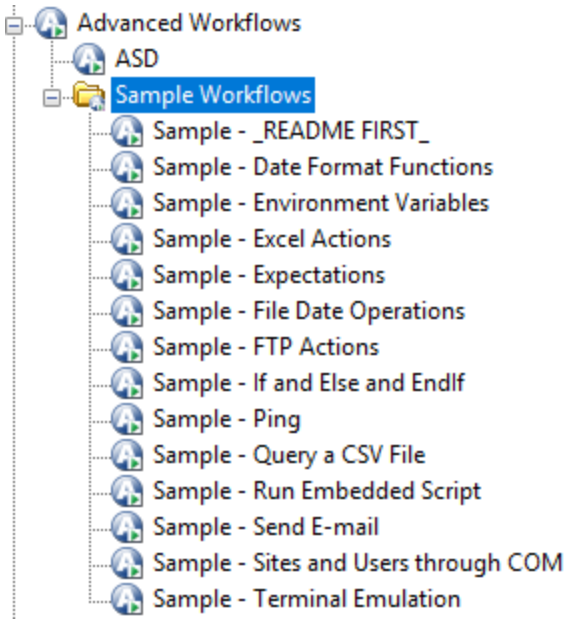


11. (Optional) In the **Advanced Options** area:
    - Select the **Terminate the process** check box and specify the number of seconds after which to terminate the Workflow if it fails to execute.
    - Select the **Retain Successful Task Logs** check box if you want to keep all successful attempts for this Workflow
    - Select the **Retain Failed Task Logs** check box if you want to keep all failed attempts for this workflow
    - Specify the location in which to save logs, if different than the default of C:\ProgramData\Globalscape\EFT Server\AWE\Temp\ (for example, in a shared location)
    - Specify the level of debug logging in the **Debug log level** box, **None**, **Minimal**, **Normal**, or **Verbose** (None is the default).
    - Click **View log folder**to view the CSV logs created by this workflow, saved in <installation_folder>\AWE\Temp. If you enable the logging, you should manually delete the files after you're done with them or create a Scheduled event in EFT to delete them automatically.

Your Workflow is now ready to insert into an Event Rule. The Auditing and Reporting module Event Rule reports will show the Advanced Workflow task name.

Creating Advanced Workflow Folders

Create folders in the Advanced Workflow node to organize workflows. For example, you might want to create a "Sample Workflows" folder, then move the Sample workflows into the new folder.



To create an Advanced Workflow folder

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, right-click the **Advanced Workflows** node, then click **New Workflow Folder**.
3. Provide a name for the folder (max value of 260 characters), keeping the name and characters simple to adhere to Windows path requirements. For example, name it "Sample Workflows" and copy the Sample workflows there.
4. One at a time, click the workflow to move, then click-and-drag it to the new folder.
   (Multiselect is not yet available for workflows.)

> **NOTE:** This functionality is also available in REST API. (Delete Sites AWE Task Folders, Get Sites AWE Task Folders, Patch Sites AWE Task Folders Post Sites AWE Task Folders).

Adding a Workflow Action to an Event Rule

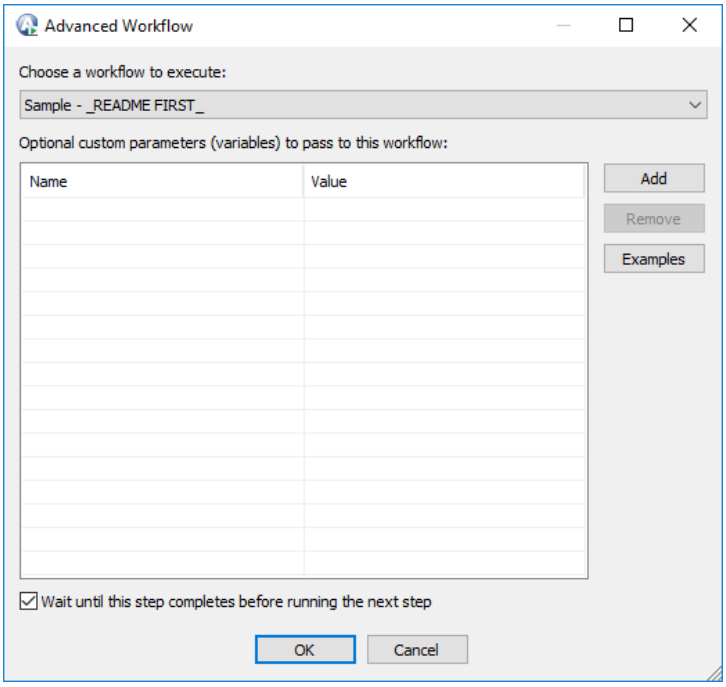
(Requires the Advanced Workflow module.) With Advanced Workflow Actions, EFT does not wait for a reply before returning control to the Event Rule thread, *unless* an "if failed" Action was specified, such as **Stop Processing this Rule**, in which case the Action waits for a return message indicating success or failure from the invoked process.

The workflows created for use in Event Rules are executed using the EFT server administrator credentials, unless you specify otherwise. If a resource cannot be accessed using the credentials under which the EFT service is running, you need to include the **optional credentials for the destination server.**

- Think of "Local Transfer" as an operation (offload or download) with a remote server.
- Think of "Optional credentials override" as "credentials to access remote server."
    - For download action, it is "credentials for source folder."
    - For copy/move (offload), it is "credentials for destination folder."
- "Credentials to access local folder" ("source" for offload and "dest" for download) is Event Rule execution context (EFT account, or Folder Monitor account for FM rules, or Connected Client account for client-originated rules on an AD site):
    - Offload: local (EFT) => remote ("override credentials")
    - Download: local (EFT) <= remote ("override credentials")
    - TEST1: Offloads file from "local" Share A (access as EFT account, i.e., X) to "remote" folder B (access as Y) => Fails, as X has no permissions on A.
    - TEST2: Downloads file from "remote" Share A (access as Y) to "local" folder B (access as EFT account, i.e., X) => Succeeds, as Y has permissions on A and X has permissions on B.

To add a Workflow to an Event Rule

1. Create a Workflow.
2. Create an Event Rule.
3. In the **Actions**list, double-click **Script: Advanced Workflow**. The Action is added to the Rule.
4. In the **Rule Builder**, click the **Advanced Workflow** link. The **Advanced Workflow** dialog box appears.



5. The defined Workflows appear in alphabetical order in the **Choose a workflow to execute**list (at the top of the **Advanced Workflow** dialog box). Click the down arrow to select a Workflow.
6. (Optional) Specify custom parameters to pass to the Workflow in the **Name** and **Value** columns, and then click **Add**.
7. (Optional) The **Wait until this step completes before running the next step** check box is selected by default.
    a. When the check box is selected, you can select the "If failed" action, and populate it with actions to run in case the rule fails.
    b. To allow the next step to run before this action completes, clear the check box. If check box is not selected, a prompt appears to confirm: "This step will be executed asynchronously (non-blocking), which means EFT won't wait for this step to be completed before running the next step. This could yield undesirable results if the next step depends on the output or

outcome of this one. Are you sure you want to make this action asynchronous?" (All actions in the IF FAILED section are lost if the parent action is switched from async to sync mode.)

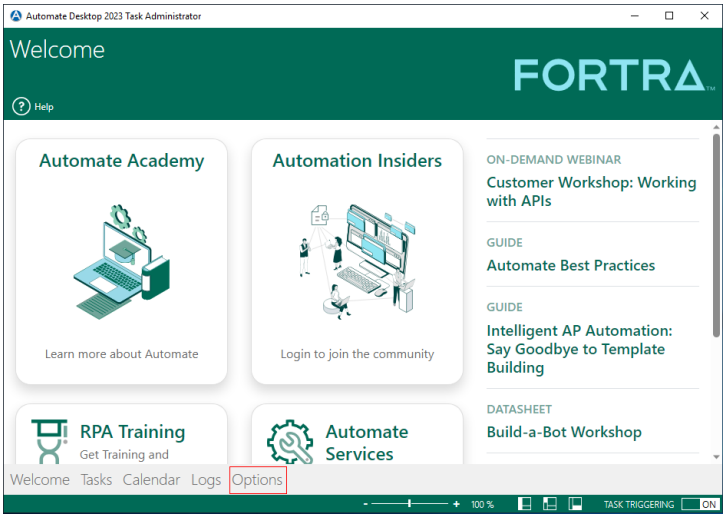
8. Click **OK**. The **Advanced Workflow** link in the **Rule Builder** updates with the name of the Workflow.
9. Add other Actions as needed, and then click **Apply** to save the changes on EFT.

Enable or Disable Running Task Window

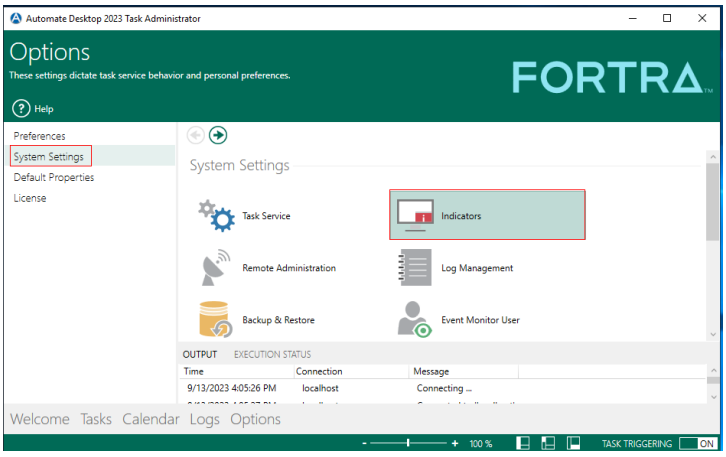
Certain Automate Actions trigger a "Task window" pop-up message that appears in the bottom right corner of the display. EFT event rules run unattended, therefore, pop-up dialog boxes are unnecessary. This functionality can have some issues with EFT environments that have multiple event rules that are triggering at any given time with continuous popups being displayed. You can enable or disable the "running task" popups in the Automate Task Administrator, as described below.

To enable or disable the running task window

1. Open the Task Administrator: **Start > Automate Desktop 2024 > Automate Desktop Task Administrator**.

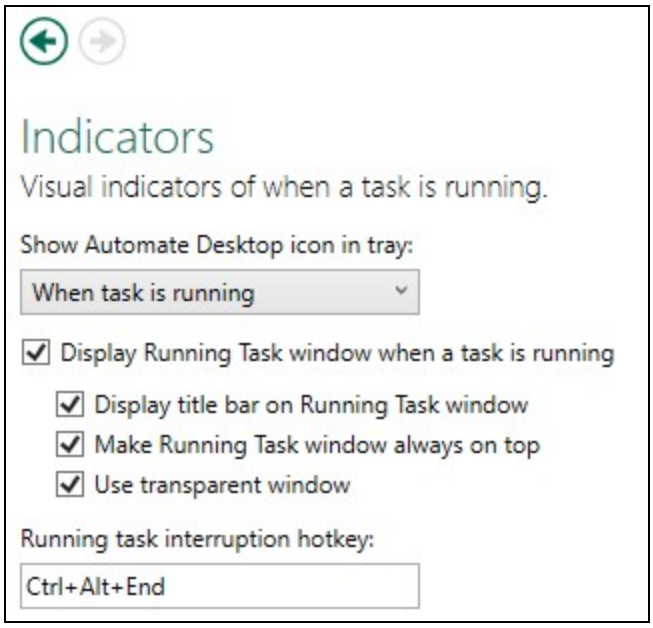


2. In the bottom menu, click **Options**.



3. In the upper left, click **System Settings**.

4. In the center of the display, double-click **Indicators**. The **Indicators** options appear.



5. Under **Show Automate Desktop icon in tray:**
   - Select (enable) or clear (disable) the **Display Running Task window when a task is running** check box.

     -OR-
   - Click the drop-down list and click **Never** instead of **When a task is running**.
6. Click **Apply**.

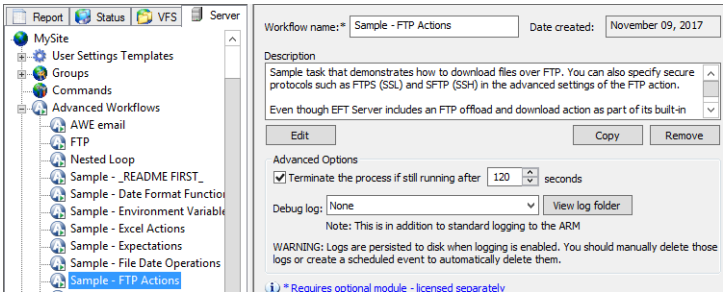
Sample Workflows

The Advanced Workflows module includes several samples to demonstrate how to create a workflow. The comments in the workflow provide instructions. The sample files are stored in **C:\ProgramData\Globalscape\EFT Server** in a database file named SiteConfig.<GUID> file (one for each Site).

> **NOTE:** In the Advanced Workflows module, variables cannot contain periods; therefore, in each variable that contains a period, the period is replaced with an underscore. For example, change `%CONNECTION.LOCAL_IP%` to `%CONNECTION_LOCAL_IP%`

To view the sample workflows

1. In the EFT administration interface, connect to EFT and click the Server tab.
2. In the left pane, expand the Site node for the Site that you want to configure, then click the Advanced Workflows node. The node expands to show the Sample Workflows.



3. In the left pane, click a sample workflow. The right pane displays the properties of the selected workflow.
4. Do one of the following to open the workflow in the Task Builder:
   - In the right pane, click **Edit**.
   - In the left pane, double-click the workflow.
5. View the comments in the Steps pane for instructions on how to configure the workflow. Use this guidance to create similar workflows.
6. If you want to save the sample workflow with your changes, click **Save and Close**. The workflow is saved in **C:\ProgramData\Globalscape\EFT Server** in a database file named SiteConfig.<GUID> file.

If you have accidentally overwritten a sample workflow and you want to revert to the original version of the sample file, you can copy the original from the default location

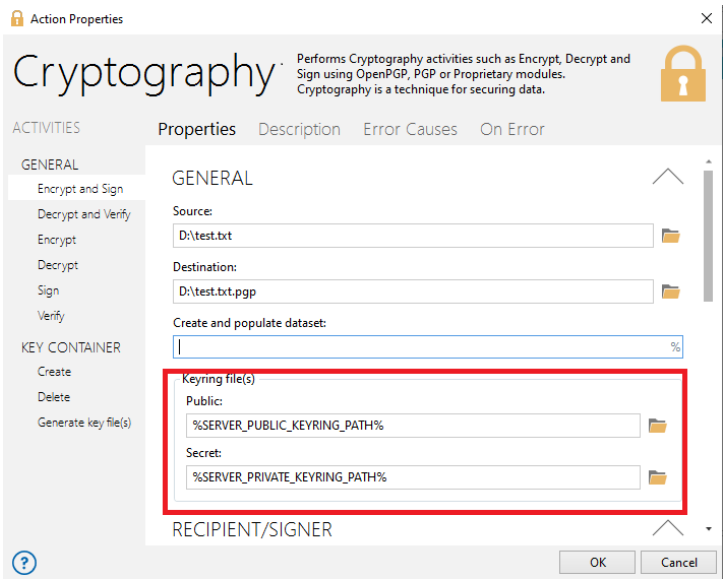
(**C:\ProgramData\Globalscape\EFT Server\AWE**). You could also make a backup copy so you don't lose the original.

Advanced Workflow Variables

Used when the Execute Advanced Workflow Action is added to an Event Rule.

Text Displayed	Variable	Description
Advanced Workflow Name	%AWE.TASK_NAME%	Workflow name
Advanced Workflow Log Path	%AWE.LOG_PATH%	Workflow log path
Advanced Workflow Error Code	%AWE.ERROR_CODE%	Workflow error code
Advanced Workflow Error Description	%AWE.ERROR_DESCRIPTION%	Workflow error description
Advanced Workflow Error Line	%AWE.ERROR_LINE%	Workflow error line
Advanced Workflow Result Code	%AWE.RESULT_CODE%	Workflow result code displayed in the Windows Event Log and others
Advanced Workflow Result Description	%AWE.RESULT_DESCRIPTION%	Workflow result description displayed in the Windows Event Log and others
Advanced Workflow Execution Time (ms)	%AWE.EXECUTION_TIME_MS%	Workflow execution time (ms)

You can also pass other EFT variables into the Advanced Workflow Actions. For example, the path to the OpenPGP keyring files can be passed to the workflow with the %SERVER_PUBLIC_KEYRING_PATH% and %SERVER_PRIVATE_KEYRING_PATH% variables.



Advanced Workflow Conditions

You can apply Advanced Workflow Conditions to any events except the Cloud-Based events.

To use one or more Advanced Workflow Conditions

1. Create the Event Rule.
2. Double-click the Condition, or click the Condition, then click **Add Condition**.
3. In the **Rule Builder**, click the hyperlinks in the Condition to specify if the Condition **does** or **does not** and **less than**, **equal to**, or **greater than** the [code], [test], or [number].
4. Then add one or more Actions and click **Apply**.

> **NOTE:** The Advanced Workflow Conditions below are available for any events except cloud-based events. They are named for their function. For example, the "If Advanced Workflow Error Description" condition will trigger the event if the Error Description in the Advanced Workflow has or doesn't have the text specified.

- If Advanced Workflow Error Code does, does not, less than, equal to, or greater than [code]
- If Advanced Workflow Error Description does, does not, equal to [text]
- If Advanced Workflow Error Line does, does not, less than, equal to, or greater than [number]
- If Advanced Workflow Result Code does, does not, less than, equal to, or greater than [code]
- If Advanced Workflow Result Description does, does not, equal to [text]
- If Advanced Workflow Execution Time does, does not, less than, equal to, or greater than [ms]

Related Topics

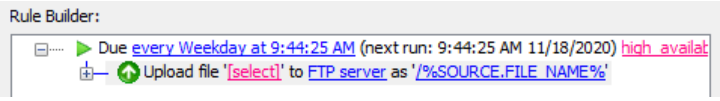
- Adding a Workflow Action to an Event Rule
- Creating Workflows for use in Event Rules

Backing Up Advanced Workflows

If you plan to edit the sample Workflows and/or create custom Workflows, you can create an Event Rule to periodically back up (save a copy of) the Workflows with a Timer rule and an Upload action.

To backup the Workflows

1. Define a Timer Rule. Specify the frequency depending on how often you create new Workflows.
2. Add the Upload action to the Rule. (Refer to Protocol: Upload Action for details.)



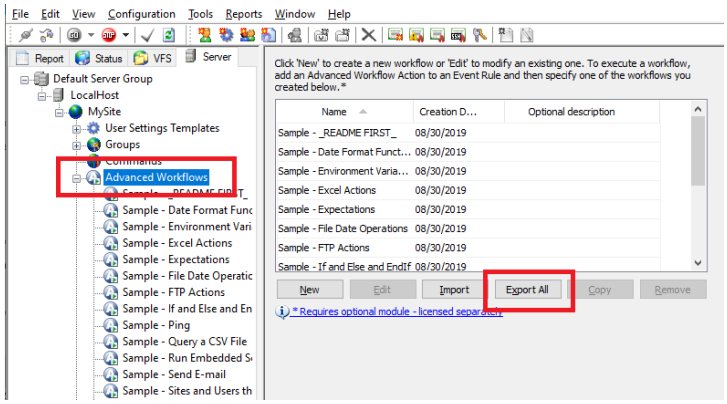
3. In the **Rule Builder**, click one of the undefined parameters (for example, '[select]' or '/%SOURCE.FILE_NAME%'). The **Upload/File Offload Configuration** wizard appears.
4. In the **Source**path box, specify the location of the Workflow (**.aml**) files. For example, to copy all of the Workflows for the Site named "MyGSSite," in the **Source path** box type `C:\ProgramData\Globalscape\EFT Server\AWE\MyGSSite_?.*`. If you use *, you will backup everything in that folder.
(Do ***NOT***select the **Delete source file**check box!)
5. In the **Destination**path box, specify a location on a remote drive (in case the local drive fails).
6. Click **Finish** in the wizard.
7. Click **Apply**.

Importing and Exporting Advanced Workflows

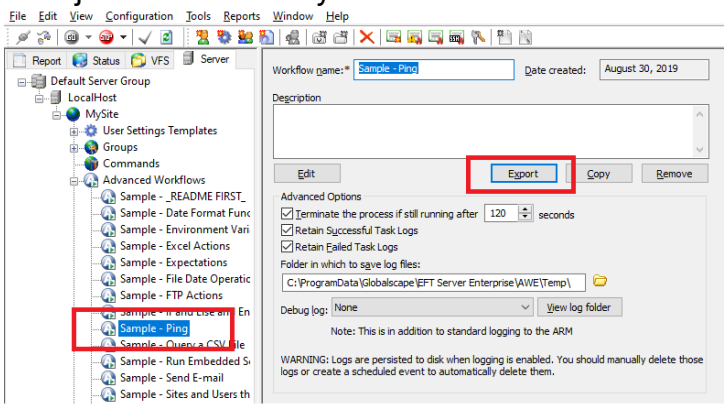
When moving an installation of EFT from staging to production, the biggest issue is moving the Event Rules. You can export the Workflows for source control, "diff" reports, interaction with support, manual editing, migrations, and so on.

> **NOTE:** After upgrading to EFT v8.2, tasks (AML files) imported from older versions of Automate (v10 or older) will be converted to Automate 2024 when imported using the **Import** button on the Advanced Workflows node interface. Imports that fail will be logged in an Advanced Workflow Module migration log with information about the conversion process so that the administrator can be aware of any issues or changes detected during conversion. If you try to import an AML with the same name as an existing AML, the **OK** button in the **Import Workflow** dialog box will be dimmed (unavailable).

You can export all of the workflows ...



... or just the one that you have selected:

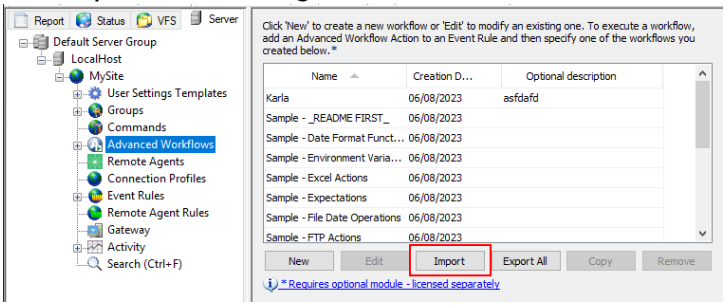


To export Advanced Workflows

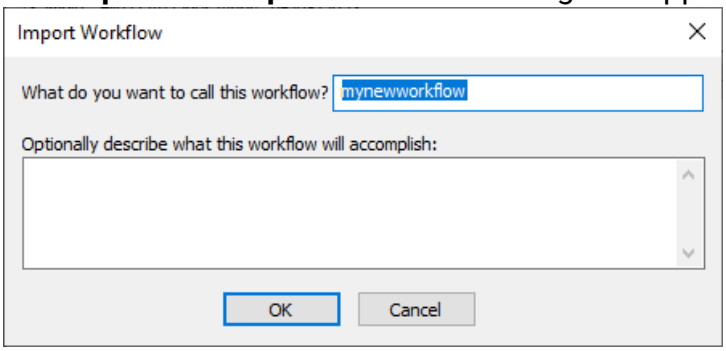
1. Click the **Advanced Workflows**node or the specific workflow that you want to export, then click **Export**. The **Browse for Folder** dialog box appears.
2. Browse for or create the folder in which you want to save the exported files, click **OK**. The AML files are saved in the specified folder.

To import Advanced Workflows

1. Click the **Advanced Workflows** node.
2. In the panel to the right of the tree, under the **Description** box, click **Import**.



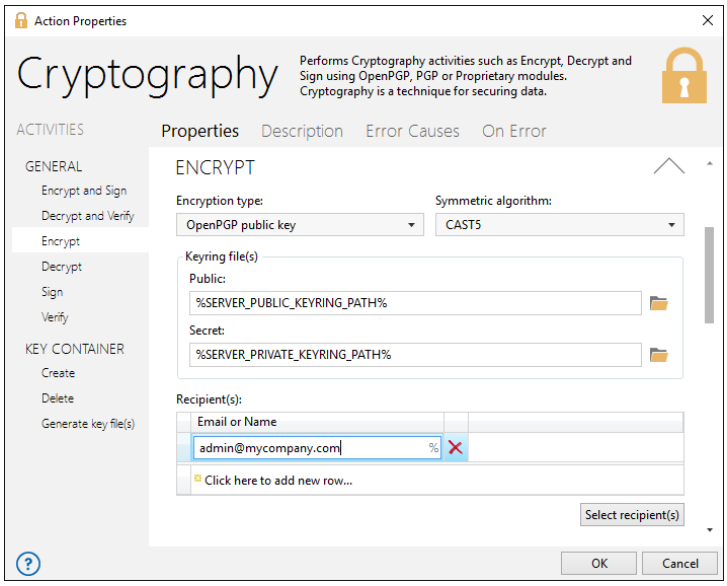
3. In the **Open** dialog box, browse for the AML file that you want to import, then click **Open**.The **Import Workflow** dialog box appears.



4. The name of the file that you imported appears in the **What do you want to call this workflow?** box. You can keep that name or change it.
5. (Optional) Provide a description of the workflow, then click **OK**.
6. The imported workflow appears under the **Advanced Workflows** node.

Encrypt Files in a Workflow Using EFT OpenPGP Key

The EFT OpenPGP keys are stored in the SiteConfig.<GUID> file. If for some reason you want to reference the keys in an Advanced Workflow instead of the EFT OpenPGP Action, you can use the Advanced Workflow Cryptography action. You can then test it in the EFT event rule (not in the Task Builder).



To encrypt files using EFT OpenPGP keys

1. Pass in the public and private keys using EFT variables (rather than an actual path): %SERVER_PUBLIC_KEYRING_PATH% and %SERVER_PRIVATE_KEYRING_PATH%.
2. Manually add the recipient by clicking **Click here to add new row** and then typing the email address that matches the one in the keyring.
    - Do NOT type **Select recipients**to find the address.
    - Do NOT test the Workflow in the Task Builder.
3. Click **OK** to save the action in the Workflow.
4. Add the Workflow to an EFT Event Rule in the EFT Rule Builder.

Related Topics

- Creating Key Pairs for OpenPGP
- Defining Event Rules
- Advanced Workflows

Technical Reference

This section provides help for the following features:

- Introduction to AML
- Arrays
- Constants
- Datasets
- Expressions
- Functions an Extended Functions

The Technical Reference in the Task Builder provide a reference for the following components:

- **AML (Automate Markup Language)** - similar to XML, AML is the primary internal language used by Automate to define and execute tasks. When you create a task using the Task Builder, you are creating a block of AML.
- **AMError** - When a task generates an error, it automatically creates a dataset called AMError, which contains details about the error.
- **AMTask** - When a task object executes within a workflow, an Automate dataset uniquely named AMTask is automatically created. This dataset contains a collection of task-related data.
- **AMTrigger** - When a task is triggered, it automatically creates a dataset called AMTrigger. This dataset contains global information about the trigger (task name, trigger date and time, computer, etc.) as well as trigger-specific datasets containing detailed information about that status that caused the trigger.
- **Basic Scripting** - Based on Visual Basic, the Basic Scripting engine extends the functionality provided by AML, giving you access to the Windows API, COM, OLE, and ActiveX objects, and a large number of functions.

Introduction to AML (Automation Markup Language)

AML (Automation Markup Language) is the primary internal language. It is a markup language similar to HTML or XML and defines a set of rules for encoding the structure, layout and contents of tasks. AML is powerful and scalable, yet its format is designed to emphasize simplicity and usability, allowing data to be easily interpreted and shared amongst experienced programmers and novices alike. AML is comprised of a variety of available actions/activities and hundreds of functions and instructions with built-in support for variables, constants and expressions.

> **NOTE:** Do not let the fact that there is an underlying "language" scare you away. The Task Builder provides an easy-to-use visual interface layer over the top of AML. It is not necessary to learn the actual internal syntax of any of these commands; this information is documented for advanced users that wish to familiarize themselves with AML. .

BASIC Scripting encompasses all available functions which may be used either as expressions inside any task step by surrounding the function in % signs, or inside a BASIC script by using the BASIC Script action. It is not necessary to use BASIC scripting to use AML. BASIC scripting is only available to extend the built-in capabilities of AML.

The code below displays a simple task as it would appear in AML format. It is comprised of 3 steps:

1. A comment step which can be used to describe what the task will do.
2. Creates a variable with the value "Hello World!"
3. Displays the variable's value in a message dialog.

```
<!--This is an optional comment. It can be used to describe
this task. -->
<AMVARIABLE NAME="Name_of_Variable" VALUE="Hello World!"
DESCRIPTION="Description of Variable" />
<AMSHOWDIALOG MESSAGE="Hello World!" WINDOWTITLE="Message Box
Title" POSITION="lower_left" ICON="information" />
```

Arrays

Like variables, arrays are used to represent data in a task that may be different each time a task runs. But unlike standard variables, arrays can contain multiple rows and optionally multiple columns. You may want to think of an array as nothing more than a list, such as a shopping list, to-do list, birthday list, etc. All items in an array, like the items in a list, have a position somewhere between first and last. Items are numbered from lowest to highest in arrays, therefore, they are accessed by number. For example, to retrieve the element in Row 2, Column 10, the following expression would be entered:

```
%arrayName(2,10)%
```

One & Two Dimensional Arrays

An array can be used to store a list of data read from a text file or other system containing customer data. For instance, if there are 10 customers, the array would need to have 10 rows. If the data consisted of first name, last name, and company name it would need 3 columns and would need to be a two dimensional array. An array can also be a simple list of text or numeric values (e.g., multiple rows of data, only one column), this is called a one dimensional array.

An array with only one dimension is linear. In other words, it contains a list of data that can be referenced by a number. For example if my one dimensional array named myArray had 3 values, then the syntax would be:

```
myArray(1) = value1
myArray(2) = value2
myArray(3) = value3
```

In a two dimensional array, you have both rows and columns, such as a spreadsheet. You would then need to reference a cell by row and column, like the expression below which references row 1, column 5.

```
%Myarray(1,5)%
```

Creating & Setting Arrays

The Array action contains individual activities that allow you to create or modify an array. To create an array, use the Create array activity. In the properties of this activity, you give your array a name, choose whether you want your array to be a one, two, or three dimensional array and optionally, set its values. After creating an array, you can

set its values in any task step using the Set array activity or you can re-size an array using the Resize array activity.

Examples

Sample 1

This is a simple task that associates each array with a color.

```
<AMARRAY NAME="myarray" TYPE="TEXT" ROWS="3" />
<AMSET VARIABLENAME="myarray(1)">Red</AMSET>
<AMSET VARIABLENAME="myarray(2)">Blue</AMSET>
<AMSET VARIABLENAME="myarray(3)">Green</AMSET>
<AMSHOWDIALOG>%myarray(1)%
%myarray(2)%
%myarray(3)%</AMSHOWDIALOG>
```

Sample 2

This is a more complex task that uses functions and performs loops (requires a folder called C:\test\ with a few files in it).

```
<AMVARIABLE NAME="thefilename"></AMVARIABLE>
<AMVARIABLE NAME="counter"></AMVARIABLE>
<AMARRAY NAME="myarray" TYPE="TEXT" ROWS="%FileCount
('c:\test\')%" />
<AMLOOP TYPE="FOLDER" FOLDER="c:\test\"
RESULTVARIABLE="thefilename">
<AMINCREMENTVARIABLE RESULTVARIABLE="counter" />
<AMSET VARIABLENAME="myarray(%counter%)">%thefilename%</AMSET>
</AMLOOP>
<AMLOOP TOTALLOOPS="%UBound(myarray, 1)%"
RESULTVARIABLE="counter">
<AMSHOWDIALOG>%myarray(counter)%</AMSHOWDIALOG>
</AMLOOP>
```

What are Constants?

Like variables, constants are used to identify data in a task. However, unlike a variable, a constant is an identifier whose associated value is "fixed," therefore, it cannot typically be altered by a task during its execution. The elements of a constant consists of a name and value. A constant's defined value is global, thus, are available to all tasks on a particular system. When you modify a constant's value, every occurrence of that value is updated across the system.

Constants are useful for defining values that are used often but may change over time or modifying multiple instances of a value at one time. For example, you could create a constant named `AdminEmail` and assign the network administrator's email address as the value. You could use this constant in multiple tasks where you wanted to send an e-mail notification to the network administrator. If you wanted to run such a task at another location with a different network administrator, you would set up a constant of the same name at the other location and assign it whatever value you wanted. If the network administrator's e-mail address changed, you would simply change the value of the constant.

Using Constants

Constants may be used in any step parameter by specifying the name of the constant surrounded by percent (%) signs. For example, if a constant named `BackupFolder` was initially created and given the value of an existing directory used to normally backup files, specify this directory as the destination in a Copy File action, and enter `%BackupFolder%` in the **Destination** parameter of this action.

To add a constant in an action using the Expression Builder

1. In the Properties dialog of an action, click inside any entry box then click **Insert Expression/Variable** which appears next to any entry box that accepts expressions.
2. In the Expression Builder window that appears, select the folder labeled **Constants** from the list of folders located in the bottom left pane.
3. Double-click a selection from the list of the defined constants for the local machine that are populated in the bottom right pane. This populates the top pane with the selected item. The selected item will be automatically surrounded with percent signs upon insertion, therefore, there is no need to surround the item with percent signs at this point.
4. Click **Insert** to properly insert the constant and close the Expression Builder window. For further information, refer to "Using the Expression Builder" in the Automate Desktop help.

Datasets

What are Datasets?

In the simplest terms, a dataset is any named group of records. Like variables, datasets are used to represent data in a task that may be different each time a task runs. But unlike standard variables, datasets can contain multiple rows and columns. This is useful when retrieving a collection of data, such as a database or spreadsheet, or retrieving information that describes one or more objects or items. Datasets can hold information such as medical or financial records. Datasets are also used to store information returned by applications or the operating system itself. For example, Advanced Workflows returns information about task errors (e.g., error name, number, description) via an AMError dataset. Datasets can be cataloged, which permits them to be referred to by name without specifying where they are stored.

The data in a dataset is laid out like a database table, which has a unique name and consists of columns and rows. The columns consist of pre-defined units of data, such as one item in a database or personnel data about one member of a customer list. The rows contain the actual data for the columns. An example of a simple dataset containing customer data is illustrated below. The name of the dataset is Customers. The first row (in bold) contains the unique names of the dataset columns, which in this case, describes the data type. All other rows include the actual data as described by each column.

Table: Customers

First	Last	Email	Phone
John	Brown	John.Brown@mydomain.com	626 222-2222
Steven	Goldfish	goldfish@fishhere.net	323 455-4545
Paula	Smith	ps@mycompany.org	416 323-8888
James	May	jim@supergig.co.uk	416 323-3232

Using Datasets

Datasets are accessed in the same way that one would access information in a database, by specifying the column and row where the data resides. Every dataset created and used must have a unique name, much like variables. But because datasets are more like tables (as opposed to variables, which can be thought of more like containers that hold one value), they are referenced differently than other objects. When using datasets, the unique name of the dataset must be referenced followed by the column name enclosed in percentage signs. For instance:

```
%DatasetName.ColumnName%
```

When a dataset is created, the current row is automatically set to 1 (assuming that the dataset has any data, since it is possible for a dataset to have 0 rows, such as when a SQL Query returns no data). A dataset is of minimal use, however, unless one can access the other rows. Typically, this is accomplished by using the Loop Dataset action which takes a dataset name as a parameter and automatically increments the current row with each iteration. The loop continues until all the rows have been accessed. In this way, one could make a task that performs operations on each row of the dataset while using the same expression. Using the table above as an example, one can retrieve the email address of each customer using the following expression inside a Loop Dataset action:

%Customers.Email%

Using a Loop Dataset step is not the only way to access dataset rows. It is possible to directly access a particular row of a dataset by supplying the row number within the expression. For example, if the dataset contains five rows and you need to get the data in row 2, simply enter the row number enclosed in parenthesis directly after the dataset name. For example:

%DatasetName(2).ColumnName%

Again, using the table illustrated above, if you want to retrieve the phone number specified in row 3 (in this case, Paula Smith's phone number), the following expression will do the trick:

%Customers(3).Phone%

Common Actions that use Datasets

Several actions and activities create and populate datasets. The table below describes some of those actions.

Action Name	Description
SQL Query	Queries a database and populates a dataset with the data retrieved.
Get Email	Retrieves one or more messages from the specified server and populates a dataset with the results.
SNMP Get	Populates a dataset with the data sent by the agent.

Pre-Named Datasets

In addition to datasets that are created and populated during execution of an action or activity, a collection of pre-named (or fixed field) datasets are also available which can provide more insight about the behavior of a running task, determine system states or examine other elements, such as triggers used to fire off a task or errors that were generated by a task. The table below describes some of these types of datasets.

Dataset Name	Description
AMError	Determine specific characteristics about the task error that occurred, including error code or number, error description, action/activity that generated the error, and other values.

Example using SQL Query action

The SQL Query action is an example of an action that creates and populates a dataset. The fields contained within that dataset are determined by the query that was executed. For example if the following query is executed:

```
SELECT firstname, lastname,
company from customer where
city='Los Angeles';
```

Then the following dataset would be generated:

datasetname
|--firstname
|--lastname
|--company

A record (row) is created for each record (row) that is retrieved from the server. To access this data use the Loop Dataset action to loop through the records. Inside the loop you can extract the data from the field of your choice (from the current record) by using an embedded expression such as the one that follows:

```
%mydatasetname.firstname%
```

or you could combine two fields together like this:

```
%mydatasetname.firstname + ' ' +
mydatasetname.lastname%
```

Expressions such as these can be used in any parameter in any action. The AML code to display the data in a message box would look like this:

```
<AMMESSAGEBOX MESSAGETEXT="%mydatasetname.firstname%"
WINDOWTITLE="The firstname of the current record is">
```

At runtime the text %mydatasetname.firstname% is replaced by the contents of the subject of the current record.

The percent signs (%) at the beginning and end of the variable name indicates that the text in-between the percent signs is an expressionand should not be taken literally. Instead, it is replaced with the current contents of that column in the current row at runtime.

Common Dataset Fields

Most of the fields (columns) that are returned in a dataset are dictated by the action creating and populating the dataset. For example, when using the SQL Query action, the field names are controlled by the columns returned by the query. In the SNMP Get action, the field names are dependant on the SNMP query data being returned by the agent. Nonetheless, a common set of fields are available which can be used to retrieve information about any created dataset. Most of these fields are global, which means they can be used on any dataset, regardless of which action or activity the dataset originated from. These fields can be accessed in the same manner as other fields, though some of their values are read only. Also, the values of these fields are the same regardless of the row being accessed.

The table below describes the common set of fields (columns) that a dataset creates (assuming the dataset name assigned is theDataset).

Name	Data Type	Return Value
theDataset.CurrentRow	Number	The current row that will be accessed in the dataset by an expression that does not contain a specific row index.
theDataset.TotalRows	Number	The total number of rows in the dataset
theDataset.TotalColumns	Number	The total number of columns (not including the static columns) in the dataset.
theDataset.ExecutionDate	Date	The date and time the dataset was created and populated
theDataset.RowsAffected	Number	The number of rows affected by an update.
theDataset.SQLQuery	Text	The SQL Query that was used to generate this dataset (If a SQL Query was not used, this value is empty).
theDataset.Datasource	Text	The data source used for the SQL Query, if applicable.
theDataset.ColumnNames	Text	A comma-delimited list of the column names in the dataset

Expressions

An expression, in programming, is a combination of symbols that represents a value. The expression is interpreted according to the rules of the programming language and a value is returned. The Expression Builder provides a quick and convenient way to create and evaluate BASIC expressions from directly within the parameters of a task step. Expressions work by taking the text found between percentage (%) signs and passing it to the BASIC expression interpreter. During runtime, the BASIC interpreter replaces the original expression (including the percentage signs) and returns the expression's resulting value instead.

Using Expressions

Many actions that normally require expressions may already be built into activities. However, you can use expressions to further expand an action's capabilities. For instance, you can build expressions that resolve complex, dynamic data at runtime with the use of variables, functions, extended functions and operators.

Example 1 - Simple mathematical expression

In the following example, a task runs a single step that performs a simple mathematical calculation and displays the results in a message box. To create this task:

1. In the Task Builder, add a Message Dialog activity to the Steps panel.
2. From the General properties of this activity, enter %7+7% in the Message to display parameter (as shown below) and click OK to save changes.
3. From the Task Builder's ribbon, click the Run button to start the task.

Since the phrase 7+7 is surrounded in percentage signs, knows that it should try to resolve the expression and not display it literally. To resolve the expression, at runtime, the value between the percentage signs is passed to the BASIC expression interpreter, where it is processed and the result is returned. A message dialog should appear with the value of 14 (as shown below).

Example 2 - Expression with variable

Expressions can also contain variables. Taking the previous example a step further, assume we now want the task to give the user the ability to enter a number he/she would like squared.

1. Use the Create variable activity to create a variable named NUMTOSQUARE with the initial value of 1. This variable will be used during runtime to retain the user's response to the question.
2. Use the Input dialog activity as the second step to display the question What number would you like squared? and populate the NUMTOSQUAREvariable with the answer.
3. Use a Message Dialog as the last step which will display the result by use of an expression multiplying the variable by itself. %NUMTOSQUARE *.

The complete task is displayed below in AML format. For convenience, the AML code can simply be copied and pasted directly into the Steps panel of the Task Builder.

```
<!-- Create the variable. -->
<AMVARIABLE NAME=
<!-- Ask the user to enter a number. -->
<AMINPUTBOX
<!-- Perform the calculation using an inline expression. -->
<AMMESSAGEBOX%>
```

Notes

Notice that we first had to create the variable we intend to use. All variables to be passed into a scripting language, either explicitly through the use of a BASIC script step or implicitly through the use an expression, need to be created first. You can accomplish this using the Create Variable action.

Variable names are not case sensitive; the variables are capitalized here for clarity.

Because each expression is passed to the scripting language engine, any command available from a common BASIC script is available to you for use in expressions in your step parameters. Refer to BASIC Scripting for details on these powerful commands.

Functions and Extended Functions

In computer programming, a function is predefined code which can generate various kinds of values depending on certain input from the user. Most programming languages such as VBScript come with a pre-written, built-in range of functions that perform various procedures or routines. Functions can be used as an expression in any task step, thus, adding more intelligence to a task and further broadening the functionality. Additionally, contains an extensive collection of additional functions that increase the functionality of the Scripting Engine which are called extended functions.

Function Syntax

Most functions require other parameters to properly complete a procedure or routine. The general format of a function is its name followed by any arguments contained in between parenthesis. An argument (sometimes referred to as parameters) is a value sent to the function when it is called upon. By passing an argument to a function, the function is given information to work on. A basic function would look like this:

```
FunctionName(arguments)
```

Certain functions may not need arguments to properly perform its duty. A function without arguments must include an empty set of parentheses (). For example, the Date () function returns the current system date and the Now() function returns the current date along with the time. These functions require no arguments or parameters in which they need to perform any procedures on, therefore the proper syntax are simply the functions themselves, with nothing entered in between the parenthesis. For instance, if the following syntax was entered:

```
Date()
```

The returned result would be the current date value such as 4/1/2024.

An example of a function which requires arguments is the Len() function, which returns the number of characters in a string. The syntax for this function is Len (“string”) which requires a string to be entered inside the parenthesis in which it will perform calculations on. For example, if this was entered:

```
Len(“Hello”)
```

The returned value would be 5.

Another example is the extended function, ExtractFileName(), which requires a path and filename in between the parenthesis in which it will extract the file name from. So, if the following was entered:

```
ExtractFileName(c:\
```

The returned value would be filename.txt.

An example of a function requiring more elaborate arguments is the Left() function, which returns a specified number of characters from the left side of a string. The syntax for this function is Left(“string”, length) which requires a valid string followed by the amount of characters to return inside the parenthesis. If the following was entered:

```
Left("AutoMate", 4)
```

The return value would be Auto.

Another example is the InsStr()function which returns the position of the first occurrence of one string within another. The search begins at the first character of the string. The syntax for this function is InStr(“string1”,“String2”). So, if the following was entered:

```
InStr(Hello,o)
```

The return value would be 5 signifying that the letter “o” is the fifth character in the word “Hello”.

> **NOTE:** Sample syntax for each function and extended functions can be found in the Help document.

Using Functions

Built-in VBScript functions along with extended functions can be used to return data inside any action parameter of a task that accepts expressions by surrounding the function with percent signs. This tells that the contents in between the percent signs should not be taken literally, but used as an expression instead. For example, the Len() function can be used within Message dialog activity by simply entering the following syntax in the Message to display parameter:

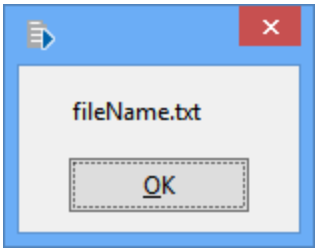
```
%Len("Hello")%
```

As previously mentioned, the Len() function returns the number of characters in a string. When the task runs, the Len() function will be performed and a message dialog displaying the results will appear, as illustrated below.

Expressions such as variables, constants or other functions can be used as arguments or parameters entered inside the parenthesis of a function. In such cases, the specified expression needs to be entered by itself (omitting any percent signs, quotes or other characters). For example, assume that a variable named %theFile% is populated with the string value c:\folderName\fileName.txt. to extract only the filename from this string and view the results in a message dialog, the proper syntax to enter in a Message Dialog step would be:

```
%ExtractFileName(theFile)%
```

During task execution, a message dialog will display the properly extracted filename as shown below.



Using Expression Builder

The Expression Builder is a valuable tool used to assist in the creation and examination of expressions. When using the Expression Builder, help regarding each function can be accessed by first selecting the Functions folder from the lower left pane, then selecting the desired function from the lower right pane and pressing the F1 key or by right-clicking the function and selecting Help from the pop-up menu that appears.

Event Rules (Automation)

The topics in this section provide the procedures for defining and using Event Rules in EFT.

- Introduction to Event Rules
- Transferring Files with Event Rules
- Event Rules Modules
- Propagating Event Rule Artifacts
- Connection Profiles
- Defining Event Rules
- Proxy Settings
- EFT Variables
- Events (Triggers)
- Actions
- Conditions

Introduction to Event Rules

Event Rules are based on a simple premise: an event occurs that triggers an action. In the EFT administration interface or with the COM API, you specify *Actions* to occur when an *Event* takes place. You can also specify one or more *Conditions* that must exist before an Action is taken or that change the Action that is taken.

For example, suppose you have a folder into which remote partners can drop files. In EFT, you can set up an Event Rule that monitors that folder, and when someone puts a file into that folder, EFT can encrypt that file, move it into another folder, and then send emails to anyone you specify informing them that a file has been moved. You can also set up a Rule that only moves certain files. For example, you can configure the Rule to move only the files with "Important" in the name, or you can route certain files to different folders.

Two administrators can work on Event Rules at the same time, but if they are working on the same Rule at the same time, when one administrator saves a Rule, when the other administrator clicks **Apply**, he will get a message saying that the changes could not be saved because changes have been made by someone else. The administrator who receives that message will have to refresh (View > Refresh or press F5) to see the other changes, and then make any changes to the Rule again.

Sample Logic

You can easily create complex programmatic Event Rules in EFT's administration interface. The Event Rule system contains objects that you click to add to the Rule builder, and then you click within the Rule to modify parameters and add variables. Below are some examples of logic you can create (in pseudo code). Refer to Events (Triggers) and Examples for examples of creating these rules in the Rule Builder.

(In the examples below, "ON FILE UPLOAD" is the Event trigger; the "if" statements are Event Rule Conditions; "PGP" and "MOVE" are Event Rule Actions.)

Always run an Action if an Event occurs:

```
ON FILE UPLOAD
{
      PGP Encrypt %FS.PATH%
}
```

Conditionally run an Action if an Event occurs (IF-THEN statement):

```
ON FILE UPLOAD
{
    if ( %FS.FILE_NAME% = "*.pgp" )
   {
      PGP Decrypt %FS.PATH%
   }
}
```

Multiple IF-THEN statements (if something, do this; if something else, do that):

```
ON FILE UPLOAD
{
  if ( %FS.FILE_NAME% = "*.pgp" )
  {
    PGP Decrypt %FS.PATH%
  }
  if ( %FS.FILE_NAME% = "*.zip" )
  {
    MOVE %FS.PATH% to
"%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\"
  }
}
```

Else statements (if preceding Condition is not met, do something):

```
ON FILE UPLOAD
{
  if ( %FS.FILE_NAME% = "*.pgp" )
  {
   PGP Decrypt %FS.PATH%
  }
  else
  {
   MOVE %FS.PATH% to
"%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\"
  }
}
```

Run always Action (Action that will always run when the Event occurs even if preceding IF-THEN-ELSE statements are true):

```
ON FILE UPLOAD
{
 if ( %FS.FILE_NAME% = "*.pgp" )
 {
  PGP Decrypt %FS.PATH%
 }
 else
 {
  MOVE %FS.PATH% to
"%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\"
 }
 MOVE "%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\*.*"
    to https://somehost/%USER.LOGON%/
 SEND NOTIFICATION email TO %user.email%
}
```

Run the same Action more than once:

```
ON FILE UPLOAD
{
 SEND NOTIFICATION email TO serveradministrator@globalscape.com
 SEND NOTIFICATION email TO %user.email%
}
```

Create compound conditional statements supporting AND and OR logical operators:

```
ON FILE UPLOAD
{
 if ( %FS.FILE_NAME% = "*.pgp" ) || ( %FS.FILE_NAME% =
"*.encrypted" )
 {
  PGP Decrypt %FS.PATH%
 }
 else
 MOVE %FS.PATH% to
"%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\"
 SEND NOTIFICATION email TO %user.email%
}
```

It is possible to configure Event Rules that create infinitely recursive cycles. A file upload Event cannot be completed until all corresponding Event Actions are finished. This could lead to unpredictable server behavior due to conflicts with shared access to the same files or deleting open files. Be careful not to create circumstances where such recursive cycles might occur. For file upload Events, recursive cycles are not typical. It is recommended that you move files on the same server using the file system, not FTP.

Transferring Files with Event Rules

You can configure EFT's Event Rules to copy, move, download, upload, or offload one file or a group of files automatically based on filename, username, location, folder changes, date or time of day, or many other variables. You can copy an entire folder structure when you offload (copy/move) files.

For details of copying or moving (offloading/pushing) a file to a specific server (host), refer to Protocol: Upload Action.

For details of downloading (pulling) a file from a specific server (host), refer to Protocol: Download Action.

Related Topics

- Monitoring Folders
- Copying or Moving a File Triggered on Folder Monitor Event and Renamed
- Copying Folder Structure When Offloading Files
- Protocol: AS2 Action
- Protocol: Download Action
- Protocol: Upload Action
- Cloud Download and Upload Actions
- Using a Command in an Event Rule to Copy Files

Event Rules Modules

Certain Event Rules functions are available in the "core" EFT, while the rest require a licensed module. The Event Rule Change Log, Event Rule Folders, Event Rule import/export, and Event Rules Permissions are part of "core" EFT.

The following Event Rule features are available without a module:

- Connection Events (all)
- File Server Events (all)
- Server Events (all)
- Site Events (all)
- "IF" and "Else" Conditions
- Backup and Cleanup Actions
- Flow: Stop Processing Action
- Flow: Variable Action
- Protocol: Email Action
- System: Backup Action
- System: Cleanup Action

The following features require a module to be licensed and registered:

<table>
<tr><td>Enterprise Actions Module (EAM)
Compression Action
CSV: Export to Dataset Action
CSV: Import from Dataset Action
File: Operation Action
Flow: Subroutine Action
Folder: Operation Action
Loop: Break Action</td><td>Loop: Dataset Action
Protocol: Listing to Dataset Action
Script: Custom Command Action
Script: PowerShell Action
Event Rule Subroutine Event
REST Invocation Event</td></tr>
<tr><td colspan="2">File Transfer Client Module (FTC)
Protocol: Download Action
Protocol: Synchronize Action
Protocol: Upload Action</td></tr>
<tr><td colspan="2">Folder Monitor Module (FMM)
Folder Monitor Event</td></tr>
<tr><td colspan="2">Timer Event Module (TEM)
Scheduler Timer Event</td></tr>
<tr><td colspan="2">OpenPGP Module (PGP)
OpenPGP Actions (Encrypt, Decrypt, Sign, Verify, SDA)
OpenSSL Actions (Sign, Verify Signature)</td></tr>
</table>

Cloud Object Monitor (CMM) • Cloud Object Monitor Event • Cloud: Download Action • Cloud: REST/Web Services Action • Cloud: Upload Action • Offload Secrets to cloud
AS2 Module (AS2) • AS2 Events
Workspaces Module (WSM) • Workspaces Events

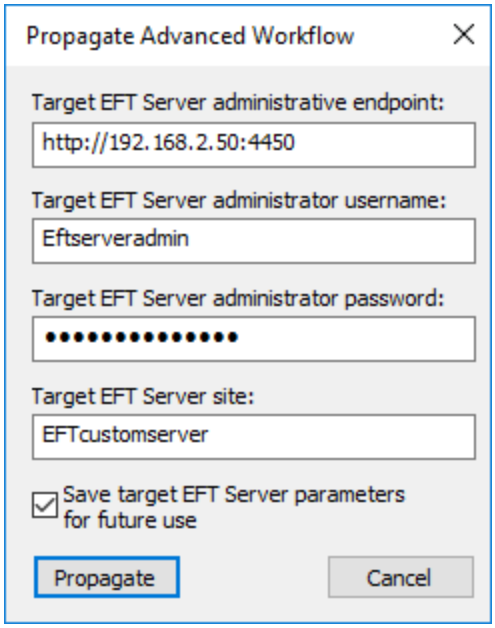
Propagating Event Rule Artifacts

Administrators can propagate (copy) individual items in Custom Commands, Advanced Workflows, and Connection Profiles to another server (for example, when adding a server to a cluster).

- Propagation is only available for EFT-managed administrator accounts
- Multiselect is not supported
- The target server must have remote administration and REST API/ web administration enabled on the **Server > Administration** tab

To propagate items

1. In the administration interface, on the **Server** tab, right-click the item to propagate (such as the Advanced Workflows node), then click **Propagate**. The **Propagate** dialog box appears.



2. In the **Propagate** dialog box, specify:
    a. **Target EFT Server administrator REST endpoint** in the form of http or htt://[host]:[port]
    b. **Target EFT Server administrator username**
    c. **Target EFT Server administrator password**
    d. **Target EFT Server Site name** to which you want to propagate the item

   a. Select the **Save target EFT Server parameters for future** use check box if you plan to propagate numerous items. All the parameters except for target server administrator password are preserved across administration interface restart.
3. Click **Propagate**. A prompt is displayed to the EFT administrator that action was successful or failed.

The result of successful propagation is that the artifact on the target EFT server is identical to the one propagated. The identity is provided by internal artifact ID.

- If target server's Site had no artifact with matching ID, it is created
- If target server's Site had the artifact with matching ID, it is replaced

Exceptions (not propagated) are:

- Custom Command's user-group assignment:
  - New Command has no user-group assignment
  - Replaced Command preserves its user-group assignment unchanged
- Advanced Workflow's Folder assignment:
  - New Workflow is placed outside any Folder
  - Replaced Workflow remains in its original Folder

> **NOTE:** In the Advanced Workflows module, variables cannot contain periods; therefore, in each variable that contains a period, the period is replaced with an underscore. For example, change `%CONNECTION.LOCAL_IP%` to `%CONNECTION_LOCAL_IP%`

- Admin ACL for all artifacts:
  - New artifact gets all admin permissions "inherited" from root container
  - Replaced artifacts preserves its permissions unchanged

When accepting the artifact, the target server performs all the standard activities, such as access control, name collision prevention, data validation, audit, logging, and so on.

- For creating new artifact, the ones performed when creating artifact via REST
- For replacing existing artifact, the ones performed when updating artifact via REST
- For name collision, no new validation was introduced, this functionality is dependent on REST API, i.e., if REST API allows it (even with case sensitivity) then propagate functionality will allow it

For artifact customization, some fields accept Run-Time Variables, which are:

- Custom Command:
    - Executable path
    - Log file path
- Advanced Workflow
    - Log directory path
- Connection Profile
    - All the fields that are Run-Time Variables-aware in Offload/Download/Cloud Actions
- Run-Time Variables are allowed to be specified in all EFT administrative interfaces (GUI, COM, and REST)
    - EFT validates incoming change and fails to accept if the fields contain unknown Run-Time Variables. In particular, it means that if the source server's artifact references the Run-Time Variable that is not defined in target server, propagation fails.

To support identity by artifact ID, EFT Administrative REST interface handles HTTP PUT requests on individual artifact endpoints.

- The new PUT REST endpoints are:
    - Custom Command: /Admin/v2/sites/<site-id>/custom-commands/<command-id>
    - Advanced Workflow: /Admin/v2/sites/<site-id>/awe-tasks/<workflow-id>
    - Connection Profile: /Admin/v2/sites/<site-id>/connection-profiles/<profile-id>
- The requests follow standard JSON:API model
- The semantics of the request is "create or replace":
    - If the endpoint corresponds to no existing artifact, EFT considers the request "create resource" one and serves it similar to POST to collection with the only difference that the artifact created has the specified (rather than random) id.
    - If the endpoint corresponds to existing artifact, EFT considers the request "replace resource" one and serves it similar to PATCH ("update resource") with the difference that, the body of PUT is considered full representation of the resource and all the missing fields are considered to have default (not "current" as for PATCH) values.

Effectively, when an artifact is propagated for the first time, target server creates its identical copy; for any subsequent propagation, target server replaces the copy with up-to-date value.

The Source server records propagation progress to EFT.log via COMMON logger (this is because the destination is not exercising REST API, its receiving incoming data).

Target server records propagation progress to EFT.log via standard REST Admin logger.

Artifact propagation is available via COM API Site interface new methods:

- ICISite::PropagateCommand
- ICISite::PropagateAdvancedWorkflow
- ICISite::PropagateConnectionProfile

Artifact propagation is available via REST Admin interface

POST REST API endpoints:

- Custom Command: /Admin/v2/sites/<site-id>/custom-commands/<command-id>
- Advanced Workflow: /Admin/v2/sites/<site-id>/awe-tasks/<workflow-id>
- Connection Profile: /Admin/v2/sites/<site-id>/connection-profiles/<profile-id>

Method name is “propagate” for all requests.

Example success case:

```
POST /Admin/v2/sites/00000000-0000-0000-0000-
000000000001/custom-commands/00000000-0000-0000-0000-
000000000001 HTTP/1.1
{
   "jsonrpc": "2.0",
   "method": "propagate",
   "id": "1",
   "params":
   {
   "targetEndpoint": "http://target:4450",
   "targetSiteName": "targetSite",
   "targetAdminUsername": "targetAdminLogin",
   "targetAdminPassword": "targetAdminPassword"
   }
}
HTTP/1.1 200 OK
{
"jsonrpc": "2.0",
```

```
"id": "1",
"result": "success"
}
```

Example failure case:

```
POST /Admin/v2/sites/00000000-0000-0000-0000-
000000000001/custom-commands/00000000-0000-0000-0000-
000000000001 HTTP/1.1
{
  "jsonrpc": "2.0",
  "method": "propagate",
  "id": "1",
  "params":
  {
  "targetEndpoint": "http://target:4450",
  "targetSiteName": "targetSite",
  "targetAdminUsername":
   "targetAdminLogin","targetAdminPassword":
   "targetAdminPassword"
  }
}
  HTTP/1.1 404 Not Found
  {
  "jsonrpc": "2.0",
  "id": "1",
  "error": {
  "code": -32004,
  "message": "Not found: custom-command (00000000-0000-0000-
0000-000000000001)"
  }
}
```

Event Rules Client Log

When EFT's **Download** and **Copy/Move** Action offloads or downloads files, the outbound session is recorded to a log file that is named **cl[yymmdd].log** (for example, **cl060312.log**) and saved in the EFT installation folder (**C:\ProgramData\Globalscape\EFT Server\Logs**). The log file is formatted as follows:

> Time; Protocol; Host Name:Port; User Name; Local Path; Remote Path; Operation; GetLastCode

For example:

```
2006-03-06 10:11:03; ftp; 192.168.20.171:21; ClientA;
 C:\test1.txt; /test1.txt; download; 226;
```

A tenth column can be added to the CL log by defining an advanced property. Refer to https://kb.globalscape.com/KnowledgebaseArticle10262.aspxfor details.

The log can be used for troubleshooting connection and transfer errors. The "GetLastCode" value returns the protocol success or error code or socket error. For example, trying to connect to a non-existent website will result in the socket error code 10060, *connection timeout*. For example, if EFT was unable to make a connection to a remote host, a code that could appear in the cl log is 10061 (connection refused). If you are using FTP to make the connection and upload/download a file, you will also see FTP Status and Error Codes. Refer to "Windows Sockets Error Codes" in the Microsoft Developer Network for a complete list of common socket error codes.

In addition to the standard socket error codes, EFT defines the socket error codes described below.

#	Description
0	Success (connected OK)
1	General socks failure
2	Socket connection not allowed by ruleset
3	The network is unreachable
4	The host is unreachable
5	The remote server actively refused the connection
6	The Time To Live (TTL) expired. This could indicate a network problem.
7	The command was not supported by the remote host. Also a catchall error code.
8	The address type or format is not supported
10	Illegal socks name
11	Socks5 authentication failure (username/password incorrect)
12	Can't connect to socks server
2000	Internal timeout error code (multiple reasons, such as firewall blocking connection, etc.)

FTP and **FTP over SSL** only return protocol-level success and error codes. For example, a successful transfer would return 226 or a bad login password would return 530. Refer to RFC 959 for a complete list of FTP/S return codes.

SFTP (SSH2) returns the following success and error codes:

#	Description
-1	Undefined or unknown error (not enough information to determine exactly why it failed) When an OpenSSH client disconnects from EFT, it reports that the exit status is **-1**. The default return code is -1, unless an optional message is returned from the server. EFT does not return the optional message, so the exit status is always -1.
0	The operation completed successfully
1	The operation failed because of trying to read at end of file
2	The requested file does not exist
3	Insufficient privileges to perform the operation
4	The requested operation failed for some other reason
5	A badly formatted message was received. This indicates an error or incompatibility in the protocol implementation
6	Connection has not been established (yet) and a timeout occurred

#	Description
7	Connection to the server was lost, and the operation could not be performed
8	A timeout occurred

Related Topics

- Introduction to EFT Logging
- Log Format, Type, and Location
- EFT in the Windows Event Viewer

Connection Profiles

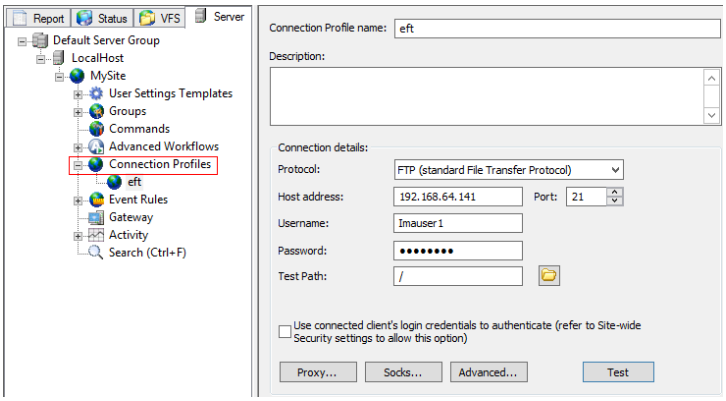
The topics below explain what Connection Profiles are and how they are used.

- Introduction to Connection Profiles
- Defining a Connection Profile

Introduction to Connection Profiles

A Connection Profile is a connection settings template to be used in Event Rules that contains the server connection settings. A profile includes the Profile Name, Description, and Connection details such as protocol, host address, credentials, proxy, socks, and so on. A **Test**button is provided to verify the specified connection options. After you've created the profile on the Site, you can specify it in Copy/Move and Download Actions so that you don't have to define it every time you create a Copy/Move or Download Event Rule. (Connection Profiles require HTTPS, SFTP, or FTPS to connect as the server.)

Connection Profiles are defined on the Connection Profiles node. Refer to Defining a Connection Profile for details.



Related Topics

- Defining a Connection Profile
- Proxy Settings Dialog Box
- Advanced Proxy Settings Dialog Box
- Using a SOCKS Proxy Server

Defining a Connection Profile

Create a Connection Profile that you can reuse in Event Rules, rather than defining external servers every time you create a new rule.

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

- Using the DMZ Gateway as a proxy is not available when using Cloud Connection profiles (Requires CCM). EFT uses the AWS SDK for cloud connections, which does not support the SOCKS protocol, which is required to proxy communications via the DMZ Gateway.
- Contact your system administrator for the proper host name, port, user name, password, and proxy type, as well as any required advanced authentication methods.

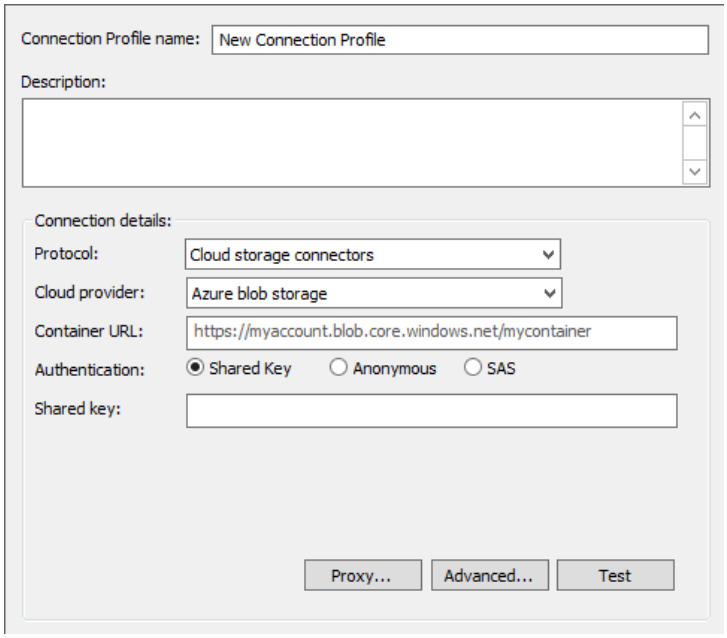
To define a Connection Profile

1. Right-click the **Connection Profiles** node, then click **New Connection Profile**.
2. In the **Connection Profile** name box, provide a name for the profile.
3. In the **Description**box, provide a description for the profile.
4. In the **Connection details** area, click the **Protocol**list to specify a protocol for the connection: Local (Local File or LAN), FTP (standard File Transfer Protocol), FTP SSL/TLS (AUTH TLS), FTP with SSL (Explicit encryption), FTP with SSL (Implicit encryption), SFTP using SSH2 (Secure Shell), HTTP (HyperText Transfer Protocol), HTTPS (Secure HTTP access), FAST - Accelerated Transfer, Cloud storage connectors.

- **Local /LAN:**

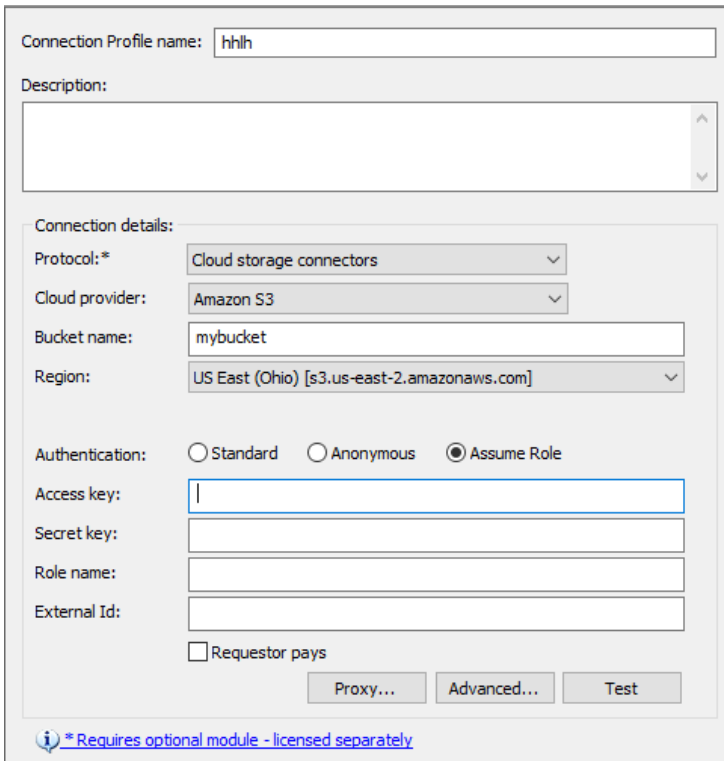
  If you selected Local (Local Files or LAN), provide the Windows account username and Password for connecting to remote shares (not local folders). These credentials are used only if/when a resource cannot be accessed using the credentials under which the EFT service is running. The **Optional credentials override**boxes allow you to specify an alternate set of logon credentials for accessing remote network shares to which the EFT service account may not have access (due to security constraints). If alternate credentials are specified, EFT will use its current security token (associated with the "Log on as" account specified in the EFT service settings) for local folder access and then new security token (associated with the alternate logon credentials) for the remote source folder accessed over network connections (e.g. network shares).

- **For Azure:**



  - Specify the **Container URL**, **Authentication**option, and **Shared key**or **SAS token**, and, if needed, Proxyand Advanced options.

- **For Amazon S3:**



- Specify the **Bucket name**, **S3 region**, **Authentication options**, **Access key**, and **Secret key**, then scroll down for Proxyand Advanced options.

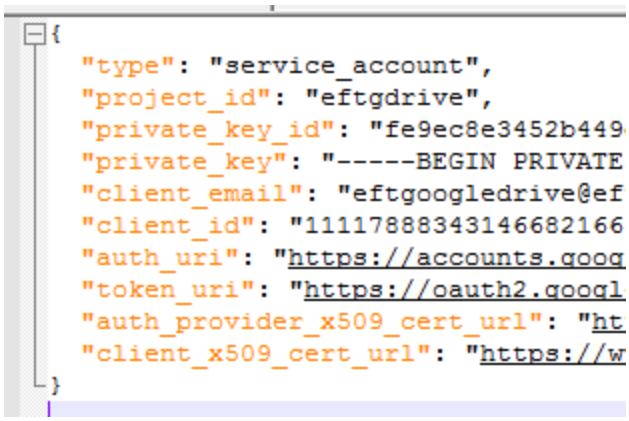
  EFT does not perform any sort of validation on the Bucket name created. Be aware of the following AWS restrictions when creating the name:

  - Bucket names can contain lowercase letters, numbers, and hyphens.
  - Each label must start and end with a lowercase letter or a number.
  - A Bucket name cannot start or end with a period.
  - Bucket names must be at least 3 and no more than 63 characters long.
  - Bucket names must not be formatted as an IP address (for example, 192.168.5.4).

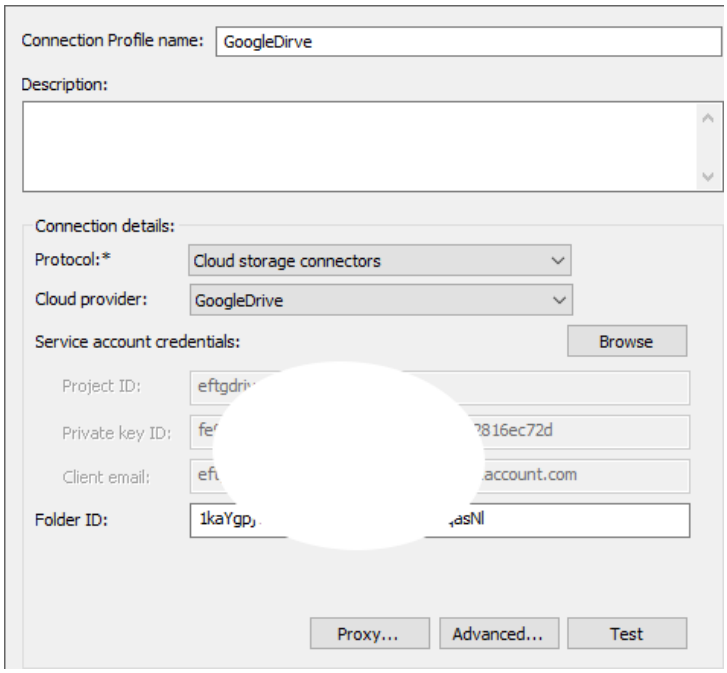
- As a best practice, always use DNS-compliant bucket names regardless of the region in which you create the bucket. For example, MyAWSBucket is a valid bucket name, even though it contains uppercase letters. If you try to access this bucket by using a virtual-hosted-style request (http://MyAWSBucket.s3.amazonaws.com/yourobject), the URL resolves to the bucket myawsbucket and not the bucket MyAWSBucket. In response, Amazon S3 will return a "bucket not found" error.
- AWS Identity and Access Management (IAM) integrates with other AWS services for comprehensive access management. To get started, set up an IAM user and define policies to control which actions that user can perform. Refer to Getting Started with AWS IAM for Beginners, Roles terms and concepts, and Create a role to delegate permissions to an AWS service for more information.
- For information regarding restrictions, limitations, and naming, refer to Creating object key names in the Amazon documentation.
- To see a list of AWS regions supported, click the **S3 region** list in the Connection profile.

- **For Google Drive:**

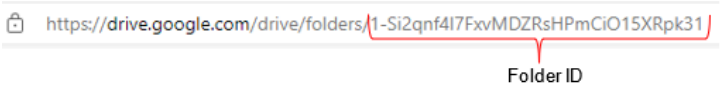
  After setting up the Google service account, download and save the service account credentials file and the JSON file generated by Google, and place the JSON file in the EFT root folder (\Program Files\Globalscape\EFT Server). The JSON is formatted similar to this:



  NOTE: Refer to https://cloud.google.com/iam/docs/service-accounts for details of Google Service accounts.



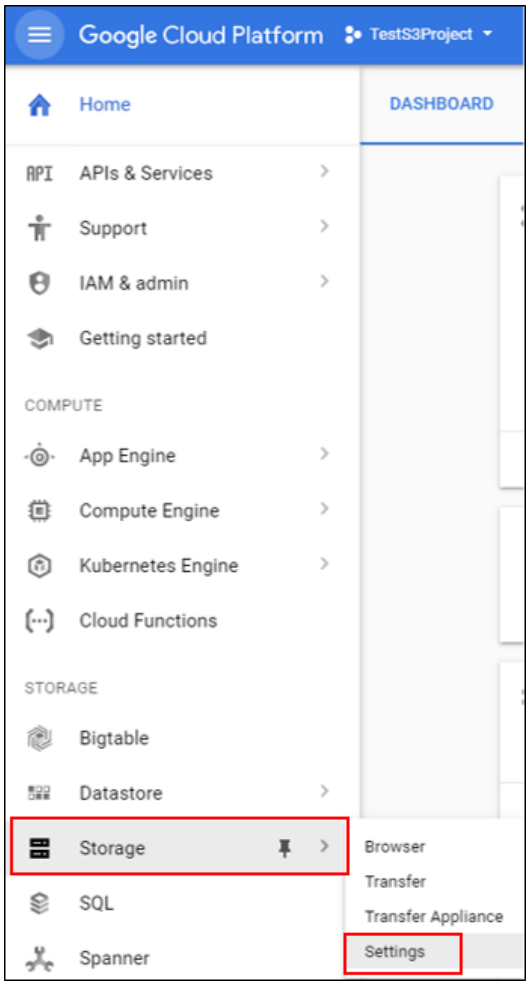
- For **Service account credentials,** click **Browse**, to find the service account credentials JSON file, downloaded from Google Cloud console. (The Google drive folder must be shared with this service account.)
- **Project ID**, **Private key ID**, and **Client email** are read-only and are completed with the service account credentials file.
- Provide the Google Drive **Folder ID**. You can get this ID by clicking on a folder in Google Drive, then copying everything after /folders/ from the URL.



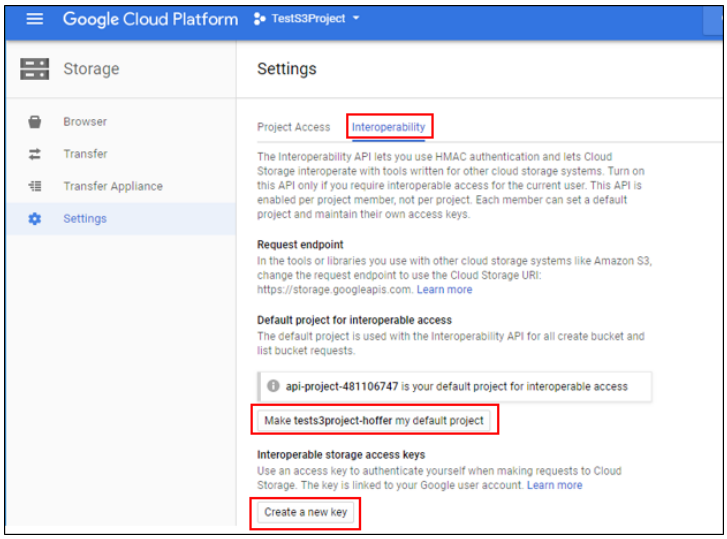
- **Alternatively, for Google Drive using Amazon S3:**

  Configure Google Cloud Storage access:

  a. Log in to Google Cloud, then click **Storage > Settings**.

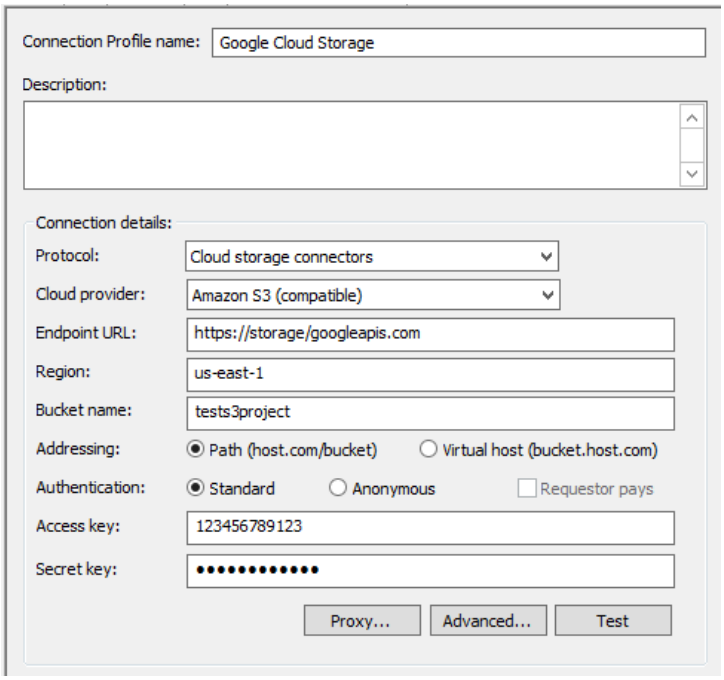


  b. In **Settings**, click **Interoperability**.



c. Under **Default project for interoperable access**, click the **Make <project name> my default project**, then click **Create a new key**.

d. In EFT, configure a Connection Profile to use the **AWS S3 (compatible)** connection:



e. Use the **Endpoint URL**https://storage/googleapis.com.

f. Specify the **Bucket name** you created in your Google Cloud Storage project

g. For **Addressing**, click Path (host.com/bucket).

h. Specify the **Access Key** and **Secret Key**as shown in your Google Cloud Storage console for "Interoperable storage access keys."

- **If you chose anything except Local or a cloud provider, do the following:**
  - In the **Host address** box, type the IP or host address of the EFT to which you want to connect.
  - The **Port**number for the selected protocol changes automatically based on the offload method. Provide a different port number, if necessary.
  - In the **Username**and **Password** boxes, type the username and password used to authenticate.
  - In the **Test Path** box, type a path to the remote folder that you will access with this Connection Profile, such as root /.
  - If you chose a protocol that uses SSL (**FTPS** or **HTTPS**), provide the client and remote server's SSL certificate information.
  - If you chose **SFTP**, provide the client SFTP certificate information.
- (Optional) Select the **Use connected client's login credentials to authenticate** check box if you want to use the local system account to authenticate. The availability of this check box is controlled by the Persist username and password credentials for use in Event Rule context variables check box on the Site's **Security**tab.
- (Optional) If you connect to EFT through a Socks server, click **SOCKS**. Refer to Using a SOCKS Proxy Server for details of configuring the SOCKS connection.
- (Optional) To configure advanced transfer options, click **Advanced**. The **Advanced Options** dialog box appears. Refer to Advanced Transfer Options for details.
- To verify the connection settings, click **Test**.

Creating Event Rules

The topics in this section provide the procedures for defining and using Event Rules in EFT.

- Defining Event Rules
- Event Rules Folders
- Event Rules Change Log
- Using Virtual Paths in Event Rules
- Using Login Credentials in Event Rules
- Using Run Now to Test and Event Rule
- Exporting and Importing Event Rules
- Managing Event Rules
- Event Rule Permissions
- Event Rules Client Log
- Advanced Transfer Options
- Event Rule Load Balancing
- SSL Options Dialog Box
- Propagating Event Rule Artifacts
- Logging Event Rule Transfer Failures
- Example: Changing the Number of Concurrent Threads Used by Event Rules
- Example: Too Many Connections per Site
- Example: Applying a Rule to a Specific User or Group
- Example: Copying or Moving a File Triggered on Folder Monitor Event and Renamed
- Example: Send an Email Notification When a Certain User Uploads a File
- Example: Copy/Move and Download File Cloud Storage Actions
- Example: Copying Folder Structure When Offloading Files
- Example: Moving an Uploaded File Based on Filename

Defining Event Rules

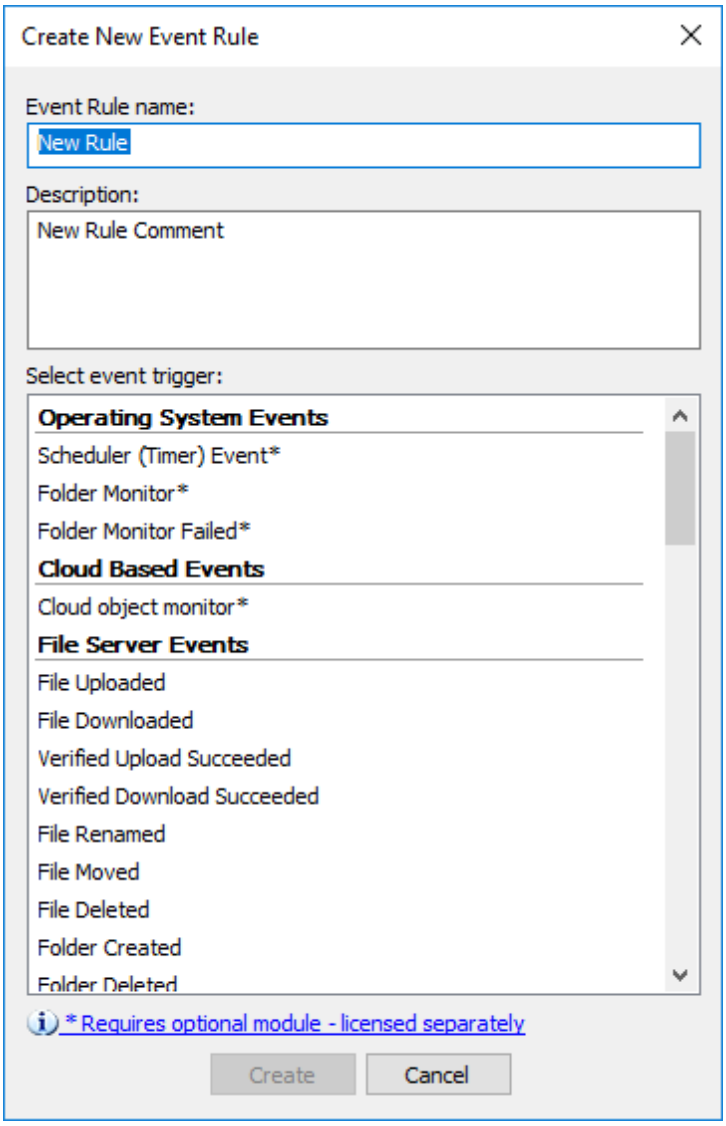
To define Event Rules in the administration interface, you begin with an Event you want to use as a trigger for the Event Rule. The Event could be when someone uploads a file, when a user quota is exceeded, when a change is detected in a folder, or many other Event triggers. Then you specify an Action to be taken when the Event occurs. The Action could be sending an email to someone, encrypting a file, moving a file, or all three together. Optionally, you can then define Conditions that must be met for the Action to be taken. You can even branch the Actions and define one Action to be taken if specified criteria are met. You do this using standard *If>Else* logic.

- While you can have two administrators working on Event Rules at the same time, if they are working on the same Rule at the same time, when they save their Rule, the second administrator to save will get a notice that the changes could not be saved because changes have been made by someone else. They then need to refresh to see the other changes, and then make their changes to the Rule again.
- The EFT log will display an error message when a file larger than 30 MB is attached to a Send notification email Action in an Event Rule.

To define an Event Rule

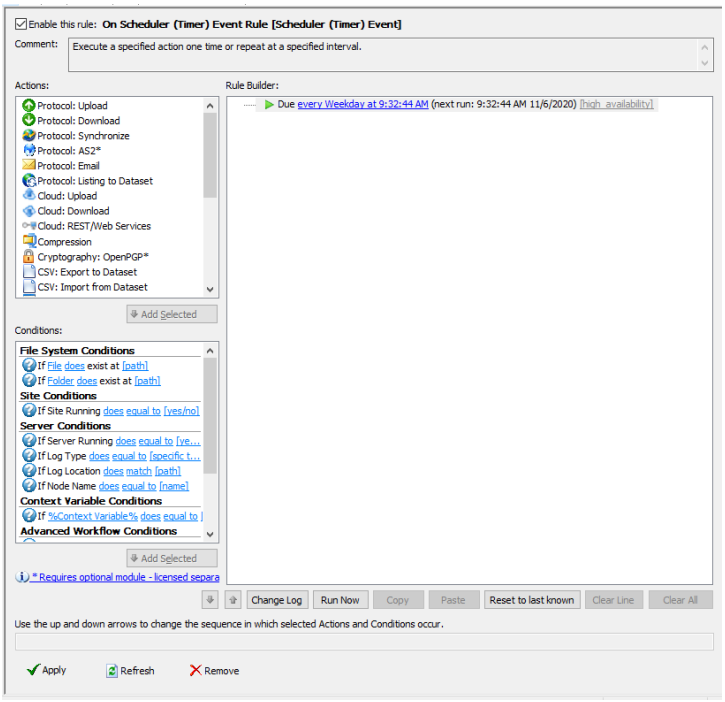
1. In the administration interface, connect to EFT and click the **Server**tab.
2. Do one of the following:
   - Right-click on the **Server**tab, and then click **New Event Rule**.
   - On the **Server**tab, expand the Site you want to configure, and then click **Event Rules**. In the right pane, click **New**.
   - On the main menu, click **Configuration >New Event Rule**.

   The **Create New Event Rule**dialog box appears.



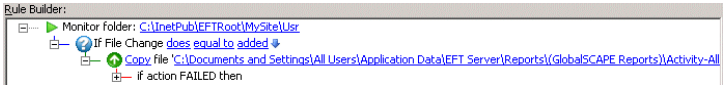
NOTE: Event triggers marked with an asterisk require a module license.

3. In the **Event Rule name** box, type a descriptive name for the Rule. This name will appear in the Event Rules node and in reports and logs. Therefore, name it something you will recognize, rather than something generic such as "Rule #24."
4. In the **Description**box, provide any notes about the Rule, such as "Periodically move and delete accounting files." You can edit these notes later in the **Comment** area for the Rule, if necessary.
5. In the **Select event trigger** box, click the Eventyou want to use as the basis of the Event Rule, such as **Folder Monitor**. For a description of the available Event triggers, refer to Events and Available Variables.
6. Click **Create**. The **Create Event New Rule**dialog box closes and the Rule Builder appears.

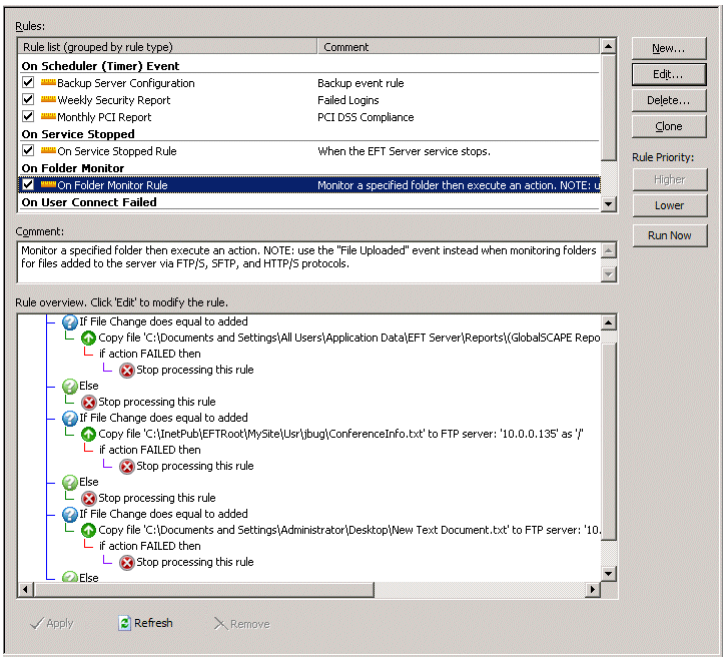


7. Actions and Conditions available for the specified event appear on the left of the Rule Builder. Conditions are optional. When applicable to the Event Rule, the Else option also appears. To add a Condition to the Rule, double-click the Condition, or click to select it, and then click **Add Condition**. Not all Conditions that EFT supports are available for every Event. To learn more about available Conditions, refer to Event Rule Conditions.
8. To add an Action to the Rule, double-click it or click the Action in the list, and then click **Add Action**. To learn more about Actions, refer to Event Rule Actions.

   As you add Conditions and Actions, they appear in the **Rule Builder**.



9. In the **Rule Builder**, click the underlined text to specify the parameters used in the definition of the Event Rule. You can also reorder the sequence of the Rule logic using the blue up/down arrows, or by clicking the Action or Condition and dragging it to the new location.
10. Click **Apply**to save the changes on EFT. EFT will not save the Rule unless it is adequately defined. Links displayed in the Rule box are parameters that must be defined before you can save and apply the Rule.
11. After the Rule is defined, click the **Event Rules** node in the Server tree in the left pane. In the right pane, each of the Rules defined on the Site appear.



12. In the right pane, in the **Rule List**, click a Rule. Comments for the Rule appear beneath the **Rule List** in the **Comment**box and the definition of the Rule (the Conditions and Actions defined) appears in the **Rule overview**box.
    - To edit the notes in the **Comment**box, click in the box and type or paste the changes.
    - To manage the Rules (edit, delete, clone, reorder), click the controls on the right. Refer to Managing Event Rules for details.
13. To delete a Rule, click to select it in the Event Rules node, and then click ✕ **Remove**at the bottom of the right pane or on the toolbar. A confirmation message appears. Click **Yes**to confirm or click **No** or **Cancel** to not delete the Rule. If clicking **Remove** doesn't work (because you were in the process of creating or changing the rule), then click **Refresh**.

Related Topics

- Managing Event Rules
- Using Login Credentials in Event Rules
- Event Rule Order of Execution
- Event Rule Examples
- List of Events
- Event Rule Conditions
- Event Rule Actions

Event Rule Folders

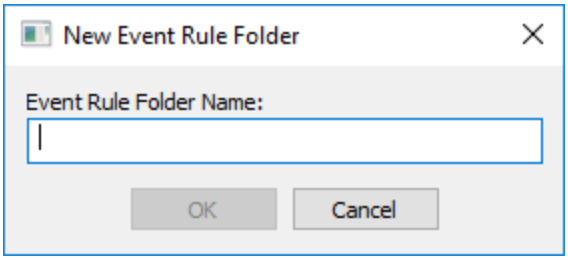
Event Rules can be organized into folders for easier management and organization.

You can:

- Apply permissions to an Event Rule folder that apply to all Event Rules in that folder.
- Create new Event Rules within a folder. (You cannot create subfolders in folders.)
- "Drag and drop" Event Rules into a folder
- Select multiple event rules and then drag them all to the new folder.

To create an Event Rule folder

1. Click the Event Rules node or an Event Rule, then click **New Event Rule Folder**. The **New Event Rule Folder** dialog box appears.



> **NOTE:** If you right-click an Event Rule and then click **New Event Rule Folder**, the selected Event Rule is NOT placed in that folder. You will have to move it if you want it to be added to the new folder.

2. Provide a name for the folder, then click **OK**.
3. Click **Apply**.
4. Now you can click and drag Event Rules into your new folder and apply any Event Rule Permissions.

Event Rules Change Log

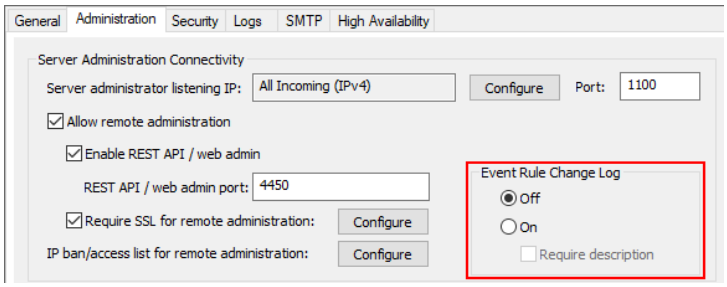
The Event Rules Change Log is used to record changes made to the Event Rules. For example, if three different administrators on three different shifts are making updates to the Event Rules or creating new Event Rules, logging these changes in the log ensures that all responsible parties are aware of the changes. Over time, this also creates a history of changes.

> **NOTE:** The Change Log only indicates changes made to existing Event Rules. It does not document the creation of an Event Rule. That is, if you've created a Rule and have never made any changes to it, it will not show up in the log.

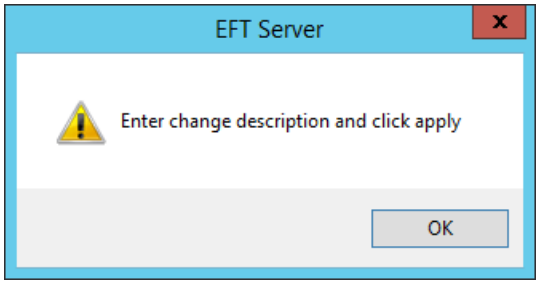
You must first enable the Change Log on the Server's **Administration**tab before changes can be recorded.

To enable and use the Change Log

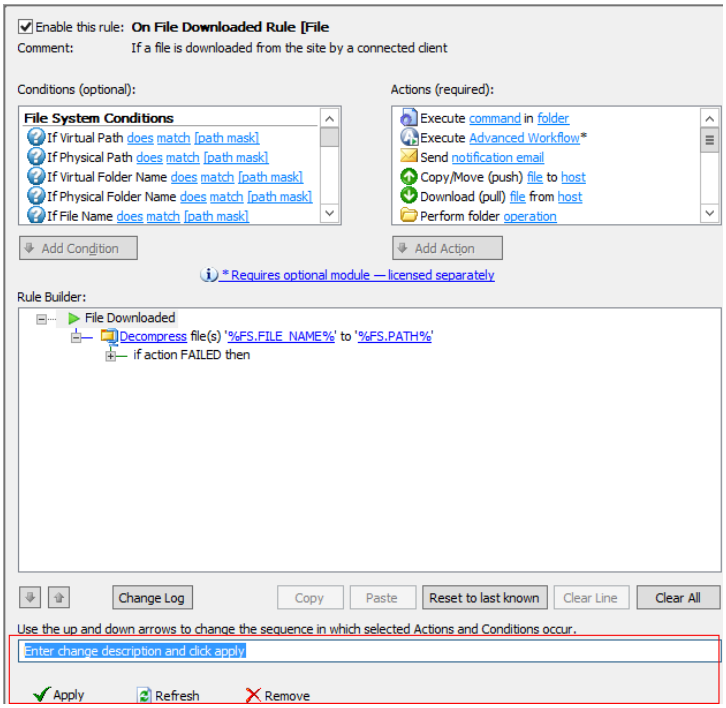
1. On the Server's **Administration**tab, under **Event Rule Change Log**, click **On**.
2. Select the **Require description** check box to require that changes contain descriptions. Without this check box selected, you can still add a description, but it is not required.



3. When the Change Log is enabled and you make a change to an Event Rule, a message appears that tells you to provide a change description.



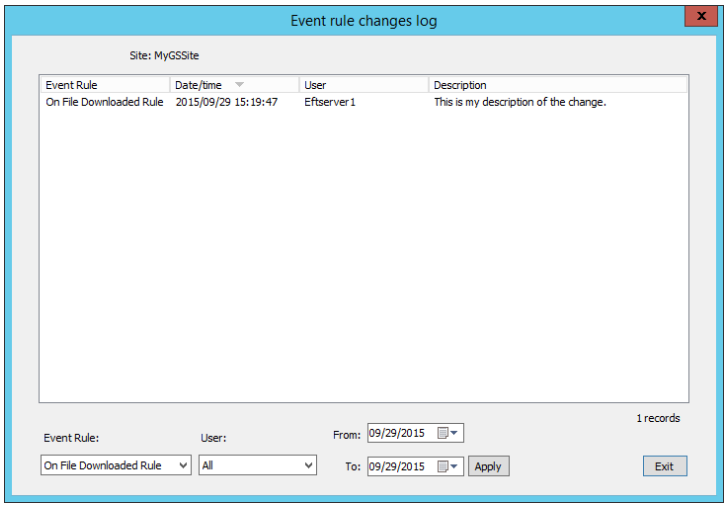
4. Click **OK**. The **Enter change description**box is enabled.



5. Provide a description of the change, then click **Apply**.

To view the Change Log

1. Open the Rule in the Rule Builder
2. Click **Change Log**. The log appears.



The log displays the name of the Event Rule, the date/time of the change, the name of the user who changed it, and the description if one was entered.

By default, only the selected Event Rule, all users, and changes on today's date are displayed. You can choose to show changes for all Event Rules, specific users, and a date range, then click **Apply**.

3. Click **Exit**when you're finished.

Using Virtual Paths In Event Rules

An EFT administrator can configure certain event rule actions using virtual paths that point to local/LAN object or cloud (AWS/Azure) objects. This allows you to configure Event Rule Actions using virtual paths that can point to local/LAN objects or cloud (AWS/Azure) storage objects. Below is a list of corresponding Event Rule Actions with paths that support the virtual path context variable (%FS.VIRTUAL_PATH%):

- Protocol: Upload,
    - Source path
- Protocol: Download
    - Destination path
    - Rename transferred file to

- Protocol: Synchronize
    - Mirror local - Source path
    - Mirror remote - Destination path
- Protocol: AS2
    - File(s) to upload
- Protocol: Email
    - Attach
- Cloud: Upload
    - Source path
- Cloud: Download
    - Destination path
    - Rename transferred file to
- Cloud: REST/Web Services
    - Save response to - File
    - Compression
- Compression
    - Source Path
    - Destination Path
- Cryptography: OpenPGP
    - File to process
- File: Scan
    - File Path
- File: Operation
    - Write operation - Destination Path
    - Read operation - Source Path
    - Rename operation - Source Path, Destination Path
    - Delete operation - Source Path
    - Concatenate operation - Source Path A, Source Path B, Destination Path
    - Checksum operation - Source Path

- Folder: Operation
    - Create action - Destination Path
    - Rename action - Source Path (Path), Destination Path (New Path)
    - Delete action - Source Path
- Script: Advanced Workflow
    - [Paths from custom parameters list] (Name/Value)

Using Login Credentials in Event Rules

User name and password variables are used by Event Rules to use a single Event Rule to support multiple users with a single Protocol: Upload Action. This allows EFT to store user name and password variables in memory for the duration of a client session. You can enable or disable this feature on the Site. **The default is disabled.**For more information on using this in an Event Rule, refer to Copy/Move File to Host Action.

To persist login credentials in memory for use in Event Rules

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Security** tab.
4. Select the **Persist username and password credentials for use in Event Rule context variables** check box.
5. Click **Apply** to save the changes on EFT.

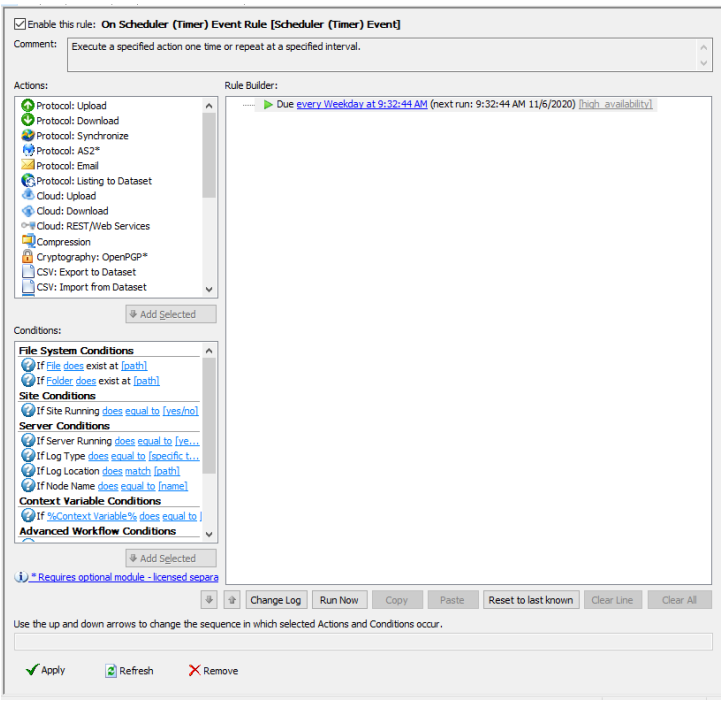
WARNING: Allowing user name and password replacement variables introduces a potential security vulnerability, because it allows passwords to reside in memory on EFT. The risk is low, but should be avoided unless you require the variables for an Event Rule.

Using Run Now to Test an Event Rule

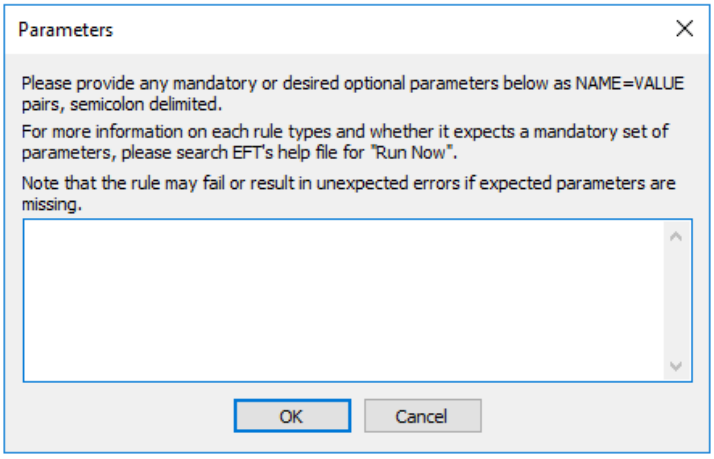
When defining Event Rules, you might want to run a quick test to verify the configuration.

To test an Event Rule

1. Define the Event Rule
2. At the bottom of the Rule Builder, click **Run Now**.



The **Parameters** dialog box appears.



3. In the **Parameters** dialog box, provide parameters that the rule is expecting, in NAME=VALUE pairs, such as USER LOGIN=lmauser1, or FS.PATH=c:\pathtomyfile\file.dot. To define multiple parameters, place a semicolon between each one.
    - Do not use percent signs % with the variables (that is, use FS.PATH, not %FS.PATH%).
    - For Folder Monitorrules, pass the following parameters when you use the "If File Change does equal to added" Condition:

      ```
      FS.MONITOR_OPERATION=added;
              FS.PATH=C:\dummyFile;
      ```

4. Click **OK**. The rule runs with the parameters used.
5. If you do not get the desired results, redefine the parameters or the rule itself and try again.

Exporting and Importing Event Rules

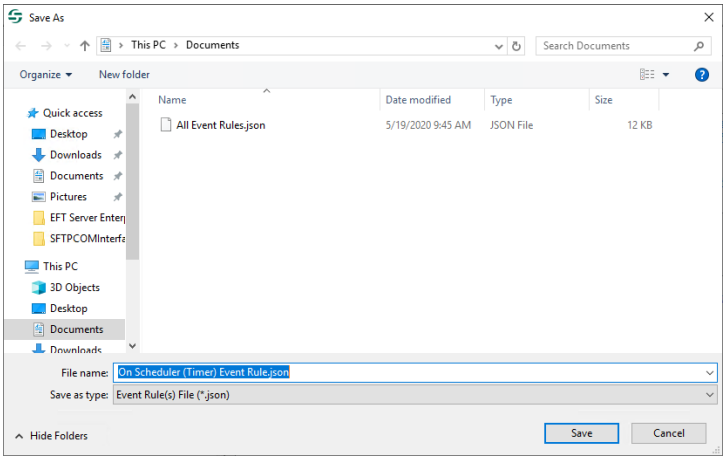
When moving an installation of EFT from staging to production, the biggest issue is moving the Event Rules.

When you do a Server Backup, all of the Event Rules are copied. Often, however, you don't want ALL of the Event Rules moved to production, just certain ones. With the import/ export feature, you can export just the Event Rules that you want as a JSON file, edit them, if needed, and importthem into another EFT installation or Site. Or perhaps you want to send the rule to a colleague or technical support for assistance. You can send someone the file, that person can review and edit as needed, and then send it back to you, and then you can import it.

- You can only export and import event rules within the same version of EFT.
- You can import a JSON file of Event Rules that contain plain-text passwords. This change applies to all fields that use passwords. Plain-text passwords in the file must be bracketed by curly braces: `{"text"}` (like normal JSON values).
- You can export one or more Advanced Workflows. Refer to Exporting Advanced Workflows.
- If you are importing a "broken" Event Rule (for example, referring to an Advanced Workflows task that does not exist), the rule will not import.
- You can also export/ import Event Rules via COM and REST API
- You cannot import empty event rule folders. (Bug 380600)

To export Event Rules

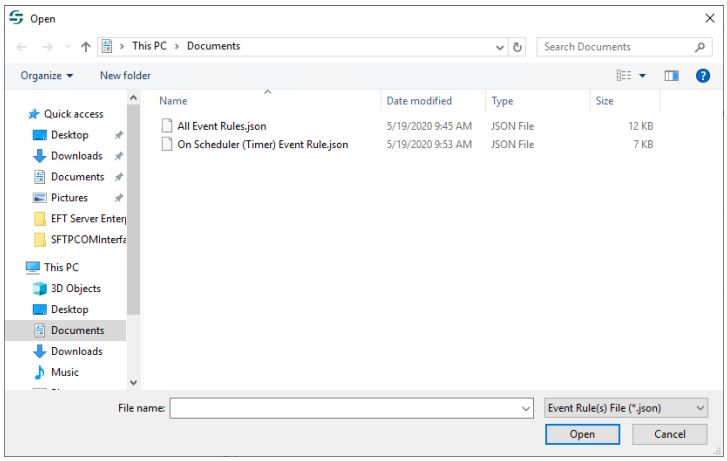
1. Right-click the Event Rule that you want to export (or the Event Rules node), then click **Export Event Rule**. The Windows **Save As** dialog box appears.



2. Click **Save**. The Event Rule is saved as a JSON file with the name you gave it. A message appears to confirm that it was saved.
3. You can view and edit JSON files in a text editor, such as Notepad.

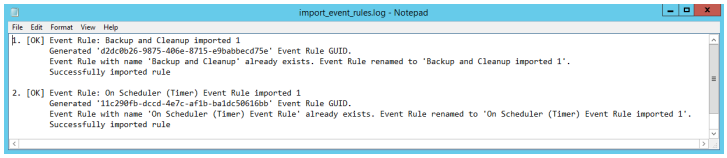
To import Event Rules

1. Right-click the Event Rule that you want to import, then click **Import Event Rule**. The Windows **Open** dialog box appears.

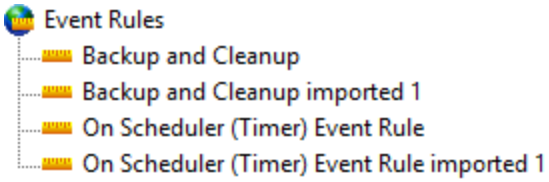


2. Click **Open**. The Event Rule is added to the Event Rules node.

   A message appears to confirm that it was imported and you are offered the option to view the log. The log file is saved to the logged-in user's \Appdata\Local\Temp\EFT folder. The Event Rule GUID, the name of the Event Rule, and success or failure of import appears in the log.



3. If an Event Rule exists with the same name as the one being imported, a number is added to the name in the tree.



4. After the Event Rule is imported, you can drag and drop it into an Event Rule folder, edit it, and so on, just like any other Event Rule.

Managing Event Rules

When you click the Event Rules node for a Site, the right pane provides controls for managing the Event Rules defined for that Site. Using this interface, you can do the following:

Edit - You can fine tune your Rules by adding, editing, deleting, and rearranging Conditions and Actions.

While you can have two administrators working on Event Rules at the same time, if they are working on the same Rule at the same time, when they save their Rule, the second administrator to save will get a notice that the changes could not be saved because the system changed underneath them. They then need to refresh to see the other changes, and then make their changes to the Rule again.

Delete - If an Event Rule is no longer needed and you are sure you will not need it again in the future, you can delete it. However, you can also disable the Rule so that, if you need the Rule again, you can simply enable it.

Clone - You can create a copy of Rule and modify it to your needs. You can then rename the Rule.

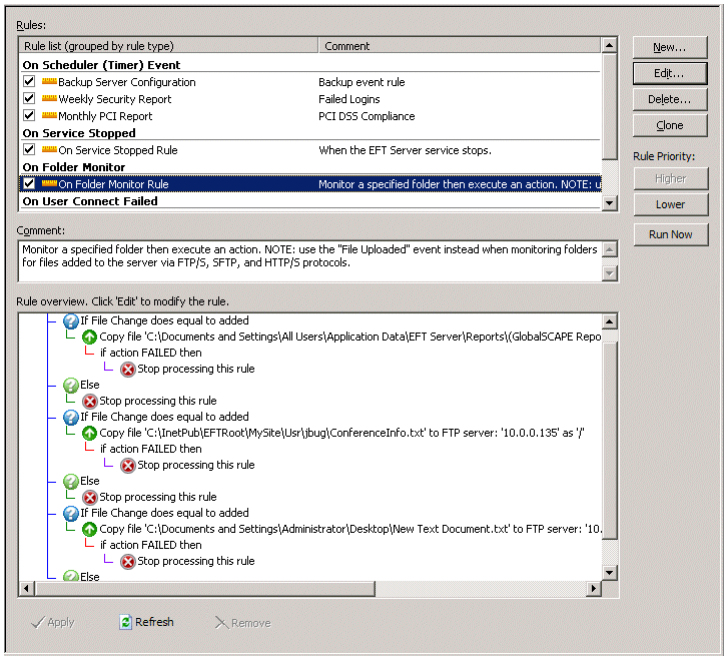
Prioritize - If you create more than one Rule for a single type of Event, EFT prioritizes the Rules in the order they appear on the Event Rules list. You can rearrange them using the **Rule Priority** buttons.

Disable - If you want to disable a Rule temporarily without deleting it, you can disable it by clearing the **Enable this rule** check box.

Rename - You can rename an Event Rule.

To manage the Event Rules

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure, and then click **Event Rules**. The list of configured Event Rules appears in the **Event Rules** node and in the right pane in the **Rule list**.



3. Click the Event Rule you want to change, and then click **Edit**, **Delete**, or **Clone**. The right pane updates to display the details specific to that Event Rule. Actions are indicated by their associated icons.

   Event triggers are indicated by a green triangle icon ▶.

   Conditions are indicated by a blue question mark icon .

   Else Conditions are indicated by a green question mark icon .

   To edit an Event Rule

   a. To add a Condition to a Rule, click a Condition from the **Conditions** list then click **Add condition**. The Condition appears in the **Rule** pane below the current highlighted insertion point. You can add multiple Conditions to a single line and create AND/OR criteria.

   b. To add an Action to a selected Condition, click it in the **Actions** list, and then click **Add action**. The Action appears in the **Rule** pane below the highlighted Condition.

   c. Configure the Condition or Action by clicking the underlined variables (red or blue underlined text)

   d. You can reorder Conditions and Actions by dragging them where you want them and using the up and down arrows.

   e. Click **Apply** to save the changes on EFT.

   To delete an Event Rule

   a. In the right pane, click **Delete**. A confirmation message appears.

   b. Click **Yes**. The Rule is deleted from the Site.

To clone an Event Rule

a. In the right pane, click **Clone**. A clone of the Rule opens in the Event Rule editing pane and is added to the **Rules** list.
b. Edit the copy of the Rule as needed, and then click **Apply** to save the changes on EFT. Your new Rule appears in the Event Rules node with "Copy" appended to the name.
c. To rename the Rule, in the left pane, right-click the Rule, and then click **Rename**.

To change the priority of a Rule

a. In the right pane, click the Rule you want to move.
b. Under **Rule Priority**, click **Higher** and **Lower**.

   Refer to Event Rule Order of Execution for details of changing the priority of a Rule.

To disable an Event Rule

a. In the right pane, clear the **Enable this rule** check box.
b. Click **Apply** to save the changes on EFT.

To re-enable an Event Rule

a. In the right pane, click the **Enable this rule** check box.
b. Click **Apply** to save the changes on EFT.

To rename an Event Rule

a. In the Event Rules node, do one of the following to make the name editable:
   - Right-click the Event Rule, and then click **Rename**.
   - Click the Event Rule, and then click it again. (Do not double-click it.)
b. Type the new name, then press ENTER or click away from the name. The name is changed.

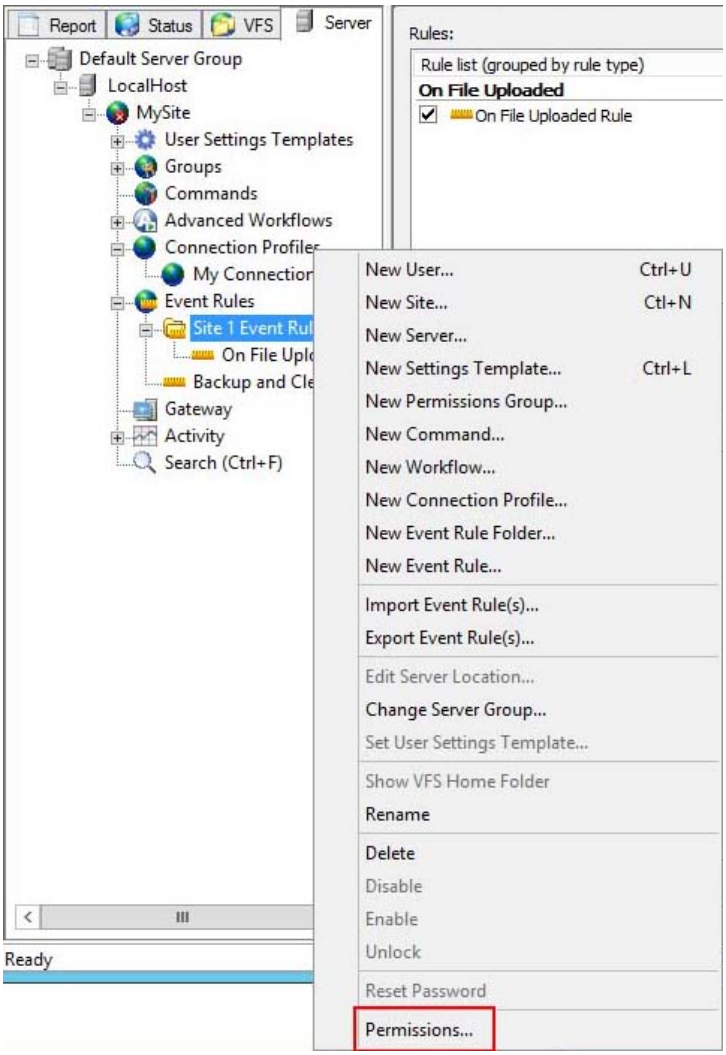
Event Rule Permissions

Permission to manage various aspects of the Event Rule system must be explicitly given to delegated administrators. Granular Event Rule permissions allow the EFT administrator to control which administrators have control over certain objects. If you change the Event Rule permissions for an administrator account while the administrator user is logged in to the administration interface, the user will have to log out and then log back in to effect the changes.

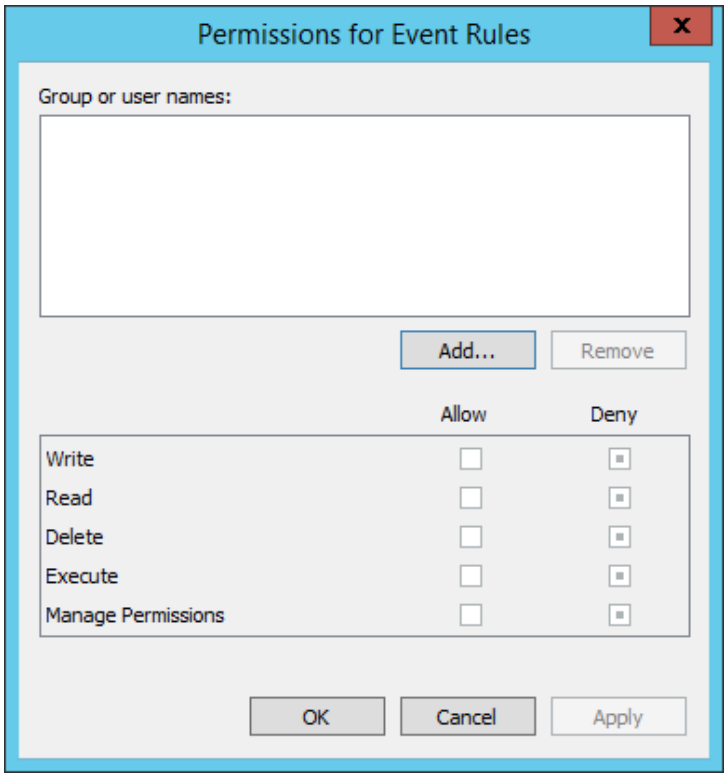
For delegated administrators to have **Allow**permission for ALL Event Rules, the Server administrator must configure permissions at the **Event Rules**node. To assign permissions only on certain Event Rule folders or only on certain Event Rules, right-click the folder or Event Rule, then click **Permissions**.

To manage permissions

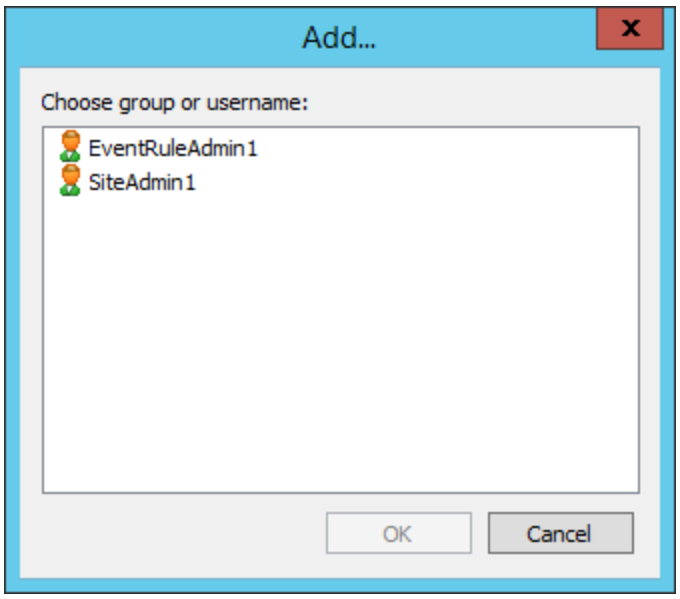
1. Log in as the **Server**administrator.
2. Right-click the Event Rules node, an Event Rules folder, an Event Rule, the Advanced Workflows node, or a Workflow, then click **Permissions**.



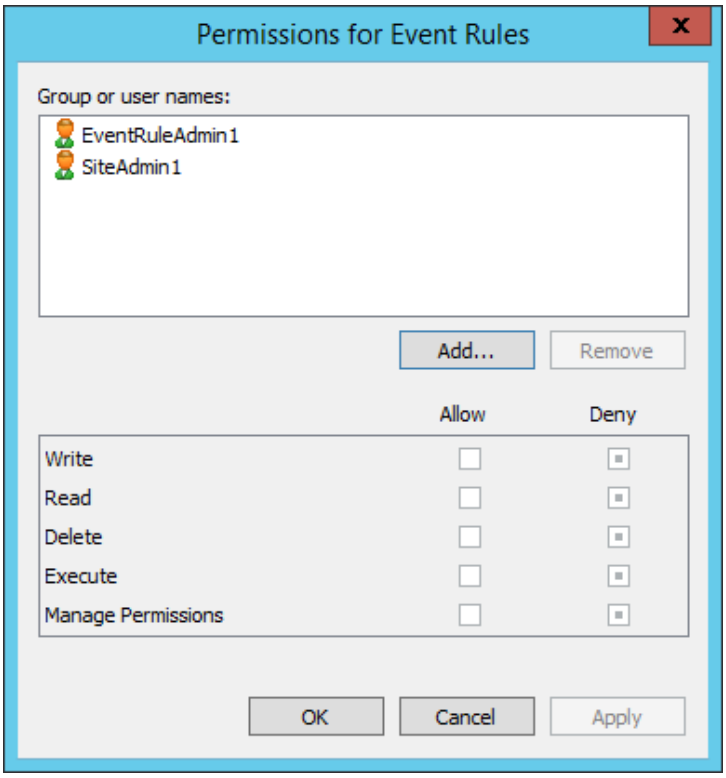
The **Permissions** dialog box appears. (The text in the title bar of the dialog box changes depending on which item in the tree you clicked.)



3. Click **Add**. Only Site and Event Rule administrators are present in the dialog box.



4. Click the administrator(s) for whom you want to add/edit permissions, then click **OK**.



5. The tristate check box for each permission has the following meanings:

Allow ☑ Deny ☐	Allowed
Allow ☐ Deny ☑	Denied
Allow ■ Deny ☐	Inherited (and allowed by inheritance)
Allow ☐ Deny ■	Inherited (and denied by inheritance)

6. Select the check boxes of the permissions that you want to **Allow** or **Deny**.
7. Click **OK**.
8. The permissions assigned at the node level and at the folder level are inherited by the items in the node or folder. You can then, as needed, edit the permissions for specific Event Rules, Workflows, or Event Rule folder.

Container Permissions

Permissions can be inherited from Container to Folder to Object. The table below describes the granular nature of these permissions.

Permission	Container	Folder	
Write	Create Folder or Object	Create Object	Update Object
Read	List	List + Show in Container List	Read + Show in Container or Folder List
Delete	None (inheritance only)	Delete this Folder	Delete this Object
Execute	None (inheritance only)	None (inheritance only)	• Execute Rule • Execute via Web-services
Manage permissions	Read and Write Permissions	Read and Write Permissions	Read and Write Permissions
Rename object requires	Write on Container or Folder + Delete on the Object		
Rename folder requires	Write on Container + Delete on the Folder		
Move rule requires:	Write on destination Container or Folder + Delete on the Rule		
Delete non-empty rule folder requires	• Delete Permission on each containing Rule • Administrator will receive “Need to Refresh” error when trying to remove/rename rules for which he/she has no Read Permission (e.g. when deleting non-empty folder containing “invisible” rules).		
Reordering rules	• Requires Delete + Manage Permissions on Container • Given an ordered set of Rules $\{R_1, R_2, \ldots, R_N\}$, of which an administrator sees $\{R_{i1}, R_{i2}, \ldots, R_{iM}\}$. If the administrator moves the Rule R_{ij}up, it will place the Rule in the complete list just before $R_{ij\text{-}1}$. Move the Rule R_{ij}down is interpreted as move the Rule $R_{ij\text{-}1}$up.		
If an administrator has no Read permission on a Command, they will not be able to	• See the Command in Choose Command list of **Execute Command Action**dialog box • Assign the Command to the Rule (for example, when applying changes to the Event Rule with the Execute Command Action configured by other administrator)		
If an administrator has no Write permission in Command Container, they will not be able to	• Create Custom Command via Event Rules interface.		
If an administrator has no Read permission on a Workflow, they will not be able to	• See the Workflow in **Choose Workflow** list of Advanced Workflow Action dialog box. • Assign the Workflow to the Rule (for example, when applying changes to the Event Rule with the Advanced Workflow Action configured by other administrator).		

Permission	Container	Folder
If an administrator has no Read permission on a Profile, they will not be able to	• See the Profile in **Choose Profile list** of Offload/Download Action wizard. • Assign the Profile to the Rule (for example, when applying changes to the Event Rule with the Offload/Download Action configured by other administrator).	

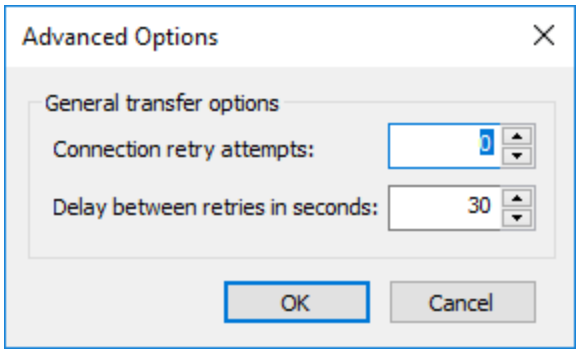
Advanced Transfer Options

The **Advanced Options** dialog box provides options for advanced transfer such as data port mode, connection retry attempts, filename encoding, time stamps, cloud transfers, and so on. These optional settings are available in the Connection Profile, File Offload configuration (Protocol Upload Action), File Download configuration (Protocol Download Action), Cloud: Upload and Download Actions, and the Web Services Action.

To configure advanced transfer options

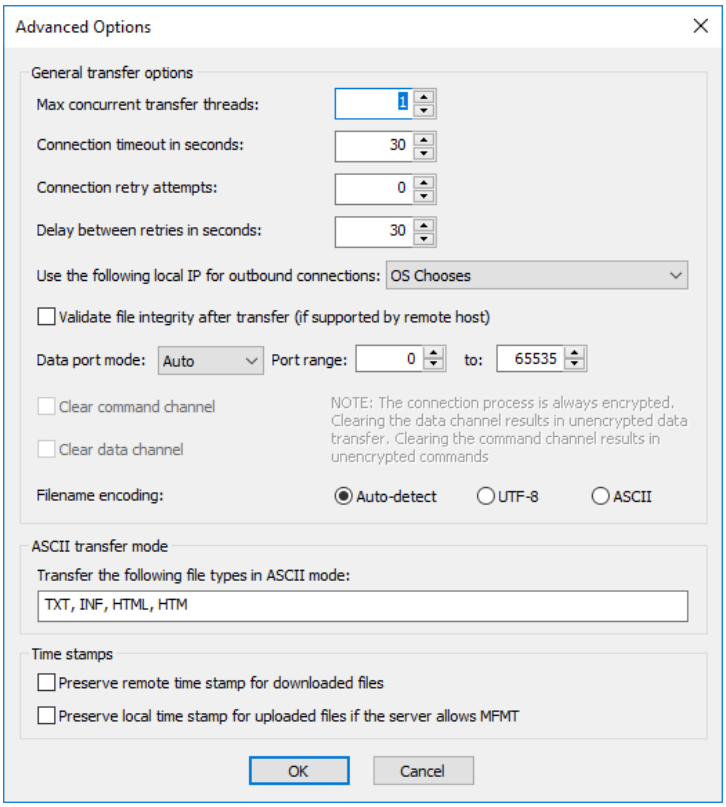
- Click **Advanced**. The **Advanced Options** dialog box appears.

For Local/LAN transfers:



- Specify the **Connection retry attempts** and **Delay between retries**. When files are being transferred with Event Rules (copy/move), if there are connection problems (for example, the network is unavailable), the server will attempt to establish a connection the number of times specified in **Connection retry attempts**. When EFT is able to re-establish the connection, it continues to transfer the file even if there are multiple interruptions.

Other protocols:



a. In the **General transfer options** area, you can provide more control over **Max concurrent transfer threads**, **Connection timeout**, **Connection retry attempts**, and **Delay between retries**. When files are being transferred with Event Rules (copy/move), if there are connection problems (for example, the network is unavailable), the server will attempt to establish a connection the number of times specified in **Connection retry attempts**. When EFT is able to re-establish the connection, it continues to transfer the file even if there are multiple interruptions.

b. Next to **Use the following local IP for outbound connections**, a list box contains an option labeled **OS Chooses** followed by a list of available IPv4 addresses and available IPv6 addresses (loopback addresses are not displayed). EFT only allows one physical IP to be selected at a time in an event rule, which cannot be replicated to the other HA nodes for obvious reasons. When the rule runs, the connection will fail on the second node with a 10038 failure, indicating that there is no IP or socket available. Click a single IP address from the list or let the operating system of EFT select the source IP based on the Site's listening IP settings. If the computer has multiple IP addresses available and/or both IPv4 and IPv6 addresses, you can specify an IP address to use or click **OS Chooses**.
    - (To specify an outbound IP address in an HA environment) In this drop-down list, you can specify a class C subnet for outbound connections. When the Event Rule executes, EFT performs a local check to see which IP addresses are available locally, and chooses the correct one based on the list selected.

c. Select the **Validate file integrity after transfer** check box to specify that EFT should double check binary files to ensure the files downloaded completely and correctly. (Not applicable to SFTP.)

d. In the **Data port mode** box, click the drop-down list and select one of the following (not applicable to SFTP):
    - **Auto**—When Auto is selected, EFT initially makes connections in PASV mode. If the PASV connection fails, EFT attempts to connect in PORT mode automatically.
    - **Active**—When Active mode is selected, EFT opens an additional port and tells the remote server to connect to <IP:PORT_RANGE> to establish a data connection. This is useful when the server is behind a firewall that closes all unnecessary ports. If you select this mode, specify the port range from which the client will choose. (For security best practices, Active mode is not allowed when brokering outbound connections through DMZ Gateway.)
    - **Passive**—When Passive mode is selected, EFT tells the remote server to provide <IP:PORT> to which EFT can connect to establish a data connection. This is useful when a client is behind a firewall that closes all unnecessary ports. Helps avoid conflicts with security systems.

e. Select the **Clear command channel** check box to send FTP commands in clear text. (Only available when FTPS is specified.)

f. Select the **Clear data channel** check box to transfer files without encryption. (Only available when FTPS is specified.)

g. In the **Filename encoding** area, specify whether the filename is encoded as **UTF-8** or **ASCII**.
   - To conserve Unicode file **names**, the remote server must support UTF-8 and advertise UTF-8 in its FEAT command.
   - To conserve Unicode file **content** you must transfer the file using binary transfer mode or save the file using UTF-8 encoding before offloading it in ASCII mode. (Refer to Knowledgebase article #11113 for more information.)
   - To enforce binary transfer mode for text files with UTF-8 encoded content, you should remove all the extensions from the **ASCII transfer mode** area in the next step or transfer files with extensions that don't match those on the ASCII types list.
   - Text (ASCII) files transferred in binary mode will retain their carriage return (CR) and line feed (LN) hidden characters which are not supported by *nix systems by default.

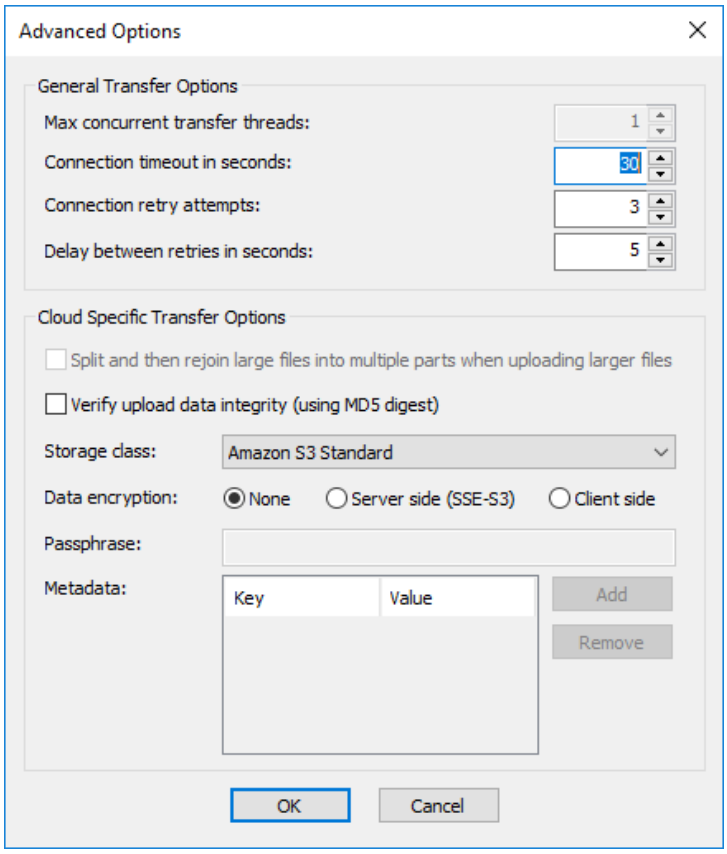
h. In the **ASCII transfer mode** area, specify the file types that can be transferred. Use a comma ***and a space*** between extensions. If you use only a comma with no space, then the Rule will not recognize the extension/file type. TXT, INF, HTML, and HTM are specified by default. If an asterisk (*) is specified, all files are downloaded in ASCII mode, even if that file doesn't have an extension. (To conserve Unicode file **content**, you must transfer the file using binary transfer mode. To force download in binary, clear the "file types" box.)

i. In the **Time stamps** area, select one of the following:
   - Select the **Preserve remote time stamp for downloaded files** check box to keep the time stamp the same on the destination file as it is on remote file.
   - Select the **Preserve the local time stamp for uploaded files if the server allows MDTM** check box to keep an uploaded file's time stamp the same on remote server as it is on the source file system. (Not applicable to SFTP.)

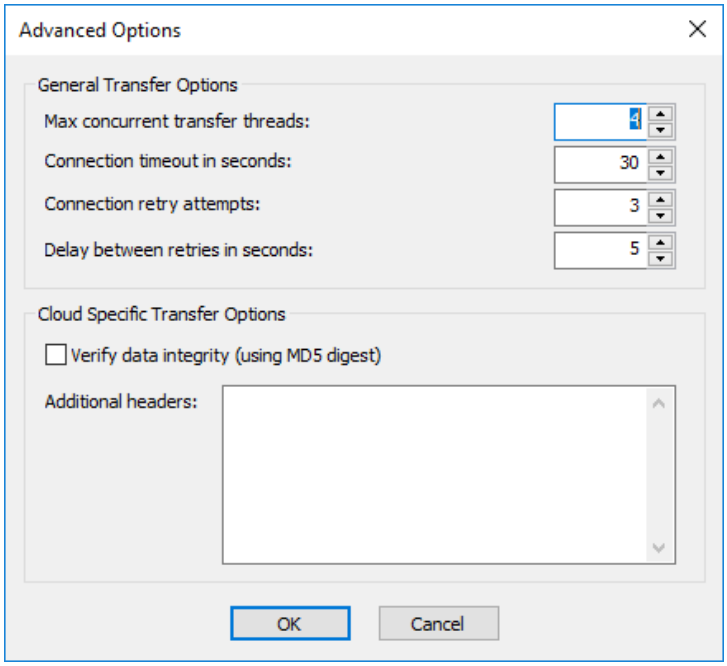
j. Click **OK**.

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

Amazon Storage:



Azure Storage:



- **General Transfer Options** are the same as above.
- If you expect large file uploads (such as video), select the **Split and then rejoin large files into multiple parts when uploading larger file**s check box.
- Select the **Verify upload data integrity (using MD5 digest)** check box to assure file integrity
- **Amazon only:**
  - In **Storage class**, specify which cloud storage to use: **Amazon S3 Standard**, **Amazon S3 Standard - Infrequent Access**, **Amazon S3 Redunancy Storage (RRS)**,
  - Data encryption options include **None**, **Server side (SS3-S3)**, and **Client side**.
  - Provide the **Passphrase** to access the storage.
  - Add any **Metadata** to capture.
- **Azure only:**
  - Additional headers: Add header information as needed, in the format header:value
- Click **OK** to save the configuration.

FAQs:

- **Can I use context variables?**

  Context variables are supported for passphrase and Metadata.

- **What is the difference between Amazon S3 vs Amazon S3 (compatible)?**

  Amazon S3 (compatible) allows you to manually specify some of the fields (Endpoint URL, Region, host format). For example, for using with S3-compatible storage, such as Google or others. (refer to Defining a Connection Profile for details)

- **Are the values in metadata passed as custom headers in the request to S3?**

  Metadata are passed as a custom header, with a name that starts with "x-amz-meta-". For example:

  ```
  x-amz-meta-metadatakey: MetadataValue
  ```

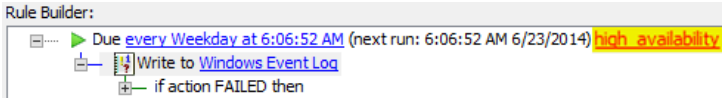
Event Rule Load Balancing

When two or more EFTs are configured in an active-active cluster, which of the EFT nodes executes a Timer or Folder Monitor Event Rule is determined by load balancing. Timer and Folder Monitor Event Rules have a "high availability" hyperlink with which you can specify if the rule will be load balanced. Clicking the hyperlink allows you to specify which node will run the Event Rule. The rule is load balanced based on which specified node is next available.

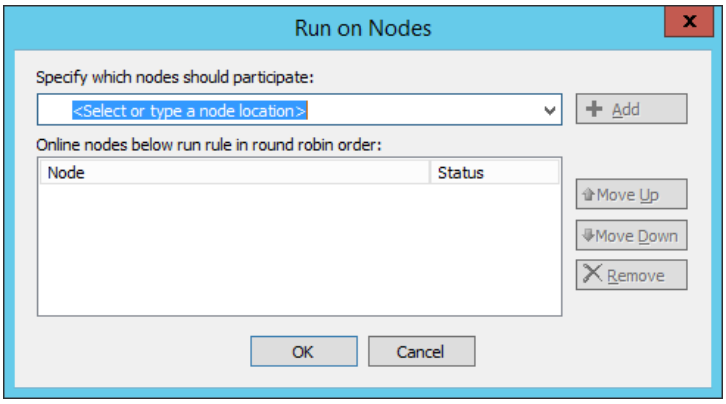
- If a specified node is offline, that node is skipped, and the rule is assigned to the next node specified in the node list. If none of the nodes specified in the list are online, an error is logged to the Windows Event Viewer.
- If you want to have a particular node handle more of the load, then you can enter that node more than once in the node list. For example, if the list is NODE1, NODE1, NODE2, NODE5, node 1 is sent Event Rules more frequently than nodes 2 or 5.
- Server Message Block (SMB) caching can cause load-balanced Folder Monitor events to fail to process files under an HA (active-active) clustered environment. To prevent this from happening, the installer creates an advanced property described in Knowledgebase article #11175: https://kb.globalscape.com/KnowledgebaseArticle11175.aspx.
- **Define a default Event Rule load balancing list, as described below**. If no nodes are specified, the rule will run in non-HA (standalone) mode in which the event runs on ALL nodes and is not load balanced. For example, a Timer rule configured to run daily at 1 pm will run on ALL nodes of the cluster every day at 1 pm. You can specify default nodes on the High Availability Tab of the Server. You can override this default policy in individual Event Rules, as shown below.

To specify nodes for Event Rule load balancing

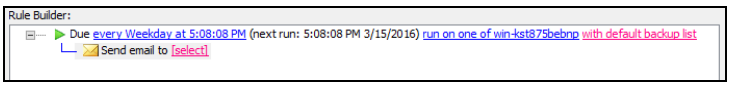
1. In the Rule Builder, in the Timer or Folder Monitor event, click the **high availability**link.



   The **Run on Nodes** dialog box appears.



2. Specify the nodes that are to run the rule (using the computer name), then click **Add**. Computer names are case sensitive. If you want a certain node to handle more of the load, list it more than once in the node list (for example, NODE1, NODE2, NODE2, NODE2, NODE 3...) You can specify nodes by IP Address (both IPv4 and IPv6).
   After you specify the nodes, the event expands to include "with default backup list."



3. Click "with default backup list" to specify the default backup list.
4. Click **OK** to save your changes in the rule.

Related Topics

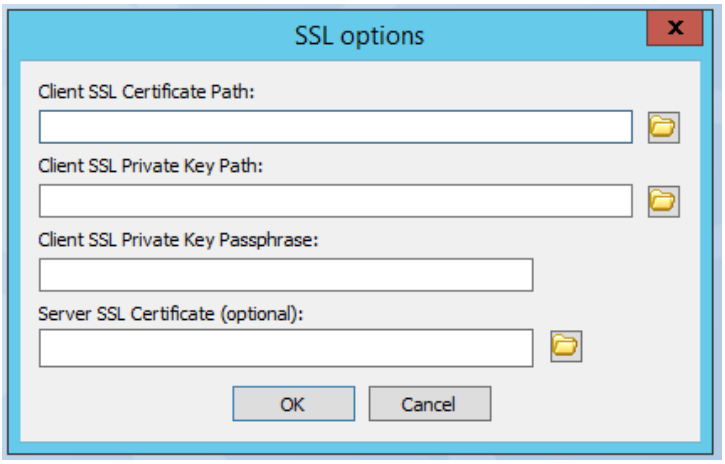
- High Availability Message Queuing
- EFT HA (Active-Active) Deployment
- High Availability Tab of a Server
- Scheduler (Timer) Event
- Folder Monitor Event

SSL Options Dialog Box

If you use a protocol that uses SSL (**FTPS**or **HTTPS**), you must provide the client and remote server's SSL certificate information in the Event Rule Action. The SSL options dialog box appears in the Connection Profile, File Offload configuration (Protocol: Upload Action), File Download configuration (Protocol: Download Action), and the Cloud: REST-Web Services Action Action.

To specify SSL options

1. In the Connection Profile or Event Rule, specify the protocol that uses SSL (**FTPS** or **HTTPS**).
2. Next to **SSL**, click **Configure**, or in the Invoke Web Service action, click **SSL**. The **SSL options** dialog box appears.



   a. In the **Client SSL Certificate Path** box, click the folder to specify the client SSL certificate path.
   b. In the **Client SSL Private Key Path** box, click the folder to specify the client SSL private key path.
   c. In the **Client SSL Private Key Passphrase** box, provide the passphrase for the client SSL certificate.
   d. In the **Server SSL Certificate**box, specify the remote server's certificate file. It is recommended, especially for production systems, that the EFT administrator obtain the remote server's SSL certificate and save it as a file in a place accessible by the EFT server service (such as the shared configuration path in HA mode or a local configuration path).

EFT will validate that the server side of any SSL-based connection made for that event action will match the server certificate. If you do not specify an SSL certificate in this box, EFT will accept any server-provided SSL certificate, which would leave the connection open to a man-in-the-middle attack.

3. Click **OK** to save the SSL options.

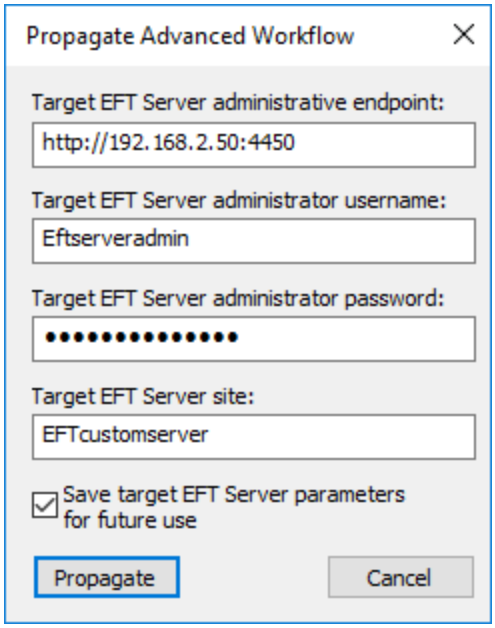
Propagating Event Rule Artifacts

Administrators can propagate (copy) individual items in Custom Commands, Advanced Workflows, and Connection Profiles to another server (for example, when adding a server to a cluster).

- Propagation is only available for EFT-managed administrator accounts
- Multiselect is not supported
- The target server must have remote administration and REST API/ web administration enabled on the **Server > Administration** tab

To propagate items

1. In the administration interface, on the **Server** tab, right-click the item to propagate (such as the Advanced Workflows node), then click **Propagate**. The **Propagate** dialog box appears.



2. In the **Propagate** dialog box, specify:
    a. **Target EFT Server administrator REST endpoint** in the form of http or htt://[host]:[port]
    b. **Target EFT Server administrator username**
    c. **Target EFT Server administrator password**
    d. **Target EFT Server Site name** to which you want to propagate the item

   a. Select the **Save target EFT Server parameters for future** use check box if you plan to propagate numerous items. All the parameters except for target server administrator password are preserved across administration interface restart.
3. Click **Propagate**. A prompt is displayed to the EFT administrator that action was successful or failed.

The result of successful propagation is that the artifact on the target EFT server is identical to the one propagated. The identity is provided by internal artifact ID.

- If target server's Site had no artifact with matching ID, it is created
- If target server's Site had the artifact with matching ID, it is replaced

Exceptions (not propagated) are:

- Custom Command's user-group assignment:
  - New Command has no user-group assignment
  - Replaced Command preserves its user-group assignment unchanged
- Advanced Workflow's Folder assignment:
  - New Workflow is placed outside any Folder
  - Replaced Workflow remains in its original Folder

> **NOTE:** In the Advanced Workflows module, variables cannot contain periods; therefore, in each variable that contains a period, the period is replaced with an underscore. For example, change `%CONNECTION.LOCAL_IP%` to `%CONNECTION_LOCAL_IP%`

- Admin ACL for all artifacts:
  - New artifact gets all admin permissions "inherited" from root container
  - Replaced artifacts preserves its permissions unchanged

When accepting the artifact, the target server performs all the standard activities, such as access control, name collision prevention, data validation, audit, logging, and so on.

- For creating new artifact, the ones performed when creating artifact via REST
- For replacing existing artifact, the ones performed when updating artifact via REST
- For name collision, no new validation was introduced, this functionality is dependent on REST API, i.e., if REST API allows it (even with case sensitivity) then propagate functionality will allow it

For artifact customization, some fields accept Run-Time Variables, which are:

- Custom Command:
    - Executable path
    - Log file path
- Advanced Workflow
    - Log directory path
- Connection Profile
    - All the fields that are Run-Time Variables-aware in Offload/Download/Cloud Actions
- Run-Time Variables are allowed to be specified in all EFT administrative interfaces (GUI, COM, and REST)
    - EFT validates incoming change and fails to accept if the fields contain unknown Run-Time Variables. In particular, it means that if the source server's artifact references the Run-Time Variable that is not defined in target server, propagation fails.

To support identity by artifact ID, EFT Administrative REST interface handles HTTP PUT requests on individual artifact endpoints.

- The new PUT REST endpoints are:
    - Custom Command: /Admin/v2/sites/<site-id>/custom-commands/<command-id>
    - Advanced Workflow: /Admin/v2/sites/<site-id>/awe-tasks/<workflow-id>
    - Connection Profile: /Admin/v2/sites/<site-id>/connection-profiles/<profile-id>
- The requests follow standard JSON:API model
- The semantics of the request is "create or replace":
    - If the endpoint corresponds to no existing artifact, EFT considers the request "create resource" one and serves it similar to POST to collection with the only difference that the artifact created has the specified (rather than random) id.
    - If the endpoint corresponds to existing artifact, EFT considers the request "replace resource" one and serves it similar to PATCH ("update resource") with the difference that, the body of PUT is considered full representation of the resource and all the missing fields are considered to have default (not "current" as for PATCH) values.

Effectively, when an artifact is propagated for the first time, target server creates its identical copy; for any subsequent propagation, target server replaces the copy with up-to-date value.

The Source server records propagation progress to EFT.log via COMMON logger (this is because the destination is not exercising REST API, its receiving incoming data).

Target server records propagation progress to EFT.log via standard REST Admin logger.

Artifact propagation is available via COM API Site interface new methods:

- ICISite::PropagateCommand
- ICISite::PropagateAdvancedWorkflow
- ICISite::PropagateConnectionProfile

Artifact propagation is available via REST Admin interface

POST REST API endpoints:

- Custom Command: /Admin/v2/sites/<site-id>/custom-commands/<command-id>
- Advanced Workflow: /Admin/v2/sites/<site-id>/awe-tasks/<workflow-id>
- Connection Profile: /Admin/v2/sites/<site-id>/connection-profiles/<profile-id>

Method name is “propagate” for all requests.

Example success case:

```
POST /Admin/v2/sites/00000000-0000-0000-0000-
000000000001/custom-commands/00000000-0000-0000-0000-
000000000001 HTTP/1.1
{
   "jsonrpc": "2.0",
   "method": "propagate",
   "id": "1",
   "params":
   {
   "targetEndpoint": "http://target:4450",
   "targetSiteName": "targetSite",
   "targetAdminUsername": "targetAdminLogin",
   "targetAdminPassword": "targetAdminPassword"
   }
}
HTTP/1.1 200 OK
{
"jsonrpc": "2.0",
```

```
"id": "1",
"result": "success"
}
```

Example failure case:

```
POST /Admin/v2/sites/00000000-0000-0000-0000-
000000000001/custom-commands/00000000-0000-0000-0000-
000000000001 HTTP/1.1
{
  "jsonrpc": "2.0",
  "method": "propagate",
  "id": "1",
  "params":
  {
  "targetEndpoint": "http://target:4450",
  "targetSiteName": "targetSite",
  "targetAdminUsername":
   "targetAdminLogin","targetAdminPassword":
   "targetAdminPassword"
  }
}
  HTTP/1.1 404 Not Found
  {
  "jsonrpc": "2.0",
  "id": "1",
  "error": {
  "code": -32004,
  "message": "Not found: custom-command (00000000-0000-0000-
0000-000000000001)"
  }
}
```

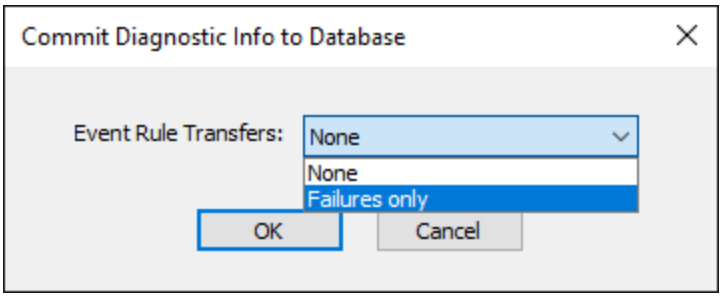
Logging Event Rule Transfer Failures

By default, and unless explicitly disabled, EFT will audit and retain all failed file transfer operations initiated by EFT's event rules to a flat file in EFT's /AppData/ directory. Optionally, you can instruct EFT to redirect its auditing of failed Event Rule-initiated transfer operations to the Auditing and Reporting (ARM) database. If enabled via this setting, those failed transfer logs will be stored in the tbl_EventRuleTransfers table in the database.

You can view a log of Event Rule transfer failures in our external business activity monitoring tool, BAM. To log more information about the failure, you must first enable the logging of failures on the **Logs** tab in EFT, as described below.

To enable and configure auditing and reporting

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node you want to configure.
3. In the right pane, click the **Logs**tab.
4. Next to **Audit event rule client outbound transfers,** click **Configure**, then specify whether to save Event Rule transfer failures to the database.



5. Click **Apply**to save the changes on the server.

Changing the Number of Concurrent Threads Used by Event Rules

Q: Is there a thread limit as to how many files can be transferred via the same Event Rule?

A: The Event Rule Monitor Folder process is limited to 3 concurrent threads by default. This means that if you have 5 Folder Monitor Event Rules monitoring the same folder, and a file is added to the monitored folder, only 3 of the 5 Rules will fire, as determined by the operating system. The 4th and then 5th Rule execute only when one or more of the first three threads are done firing and executing any Actions. If you have, for example, 100 concurrent Monitor Folder Event Rules, they are not all triggered simultaneously.

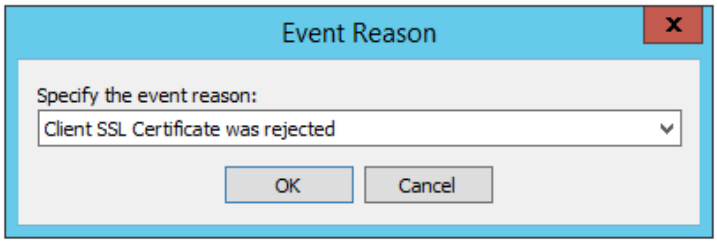
For details of overriding the default "concurrent threads" advanced property, refer to the Knowledgebase article, Changing the Number of Concurrent Threads Used by Event Rules.

Too Many Connections per Site

You can define an Event Rule to send you an email when a user login fails because there are too many connections to a Site. If the Rule is triggered frequently, you might want to change the maximum concurrent socket connections setting for the Site.

To define the Event Rule

1. Define an Event Rule using the **User Login Failed** Event trigger. The Event trigger appears in the Rule Builder.
2. In the **Conditions** list, double-click **if Event Reason** (or click it, and then click **Add Condition**) to add it to the Rule.
3. In the Rule Builder, click the linked text **[specific reason]**. The **Event Reason** dialog box appears.



4. Click the **Specify the event reason** drop-down menu to specify a reason that will trigger the Event Rule:
   - Account Disabled
   - Account Locked Out
   - Invalid password
   - Protocol not supported
   - Restricted IP
   - Too many connections per IP
   - Too many connections per Site
   - Too many connections per user

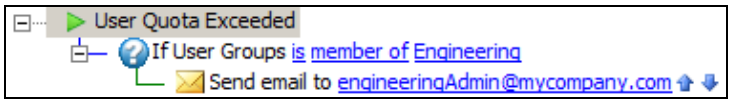
   For this example, click **Too many connections per Site**.
5. Click **OK**.
6. In the **Actions** list, double-click **Send notification email** (or click it, and then click **Add action**) to add it to the Rule.
7. In the **Rule Builder**, click the linked text **[select]**and configure an emailto send yourself a notification (or link to your defined email template) then click **OK**.
8. Click **Apply** to save the changes on EFT.

Applying a Rule to a Specific User or Group

You can use the **If User is a member of** Condition to apply the Event Rule to one or more specific Groups (By default, all Rules apply to all users.) For example, suppose the Engineering department has its own user administrator for EFT and you want the administrator to get an email when one of the user accounts exceeds its quota. You would set up a **User Quota Exceeded** Event with an **If User Groups** Condition and a **Send notification email** Action, as described below.

To create the Rule

1. Define an Event Rule using the **User Quota Exceeded**Event trigger.
2. Add the **If User Groups**Condition.
3. In the **Rule Builder**, click the **specific group(s)** link. The **Event Target Users and Groups**dialog box appears.
4. Clear the **All Users**check box and select the check box of one or more Groups to which you want this Rule to apply, and then click **OK**.
5. Add the Send notification email Action to the Rule and provide the email address of the user administrator and anyone else you want to receive the email.
6. Click **Apply**. The Rule appears similar to the following example:



Example: Copying or Moving a File Triggered on Monitor Folder Event and Renamed

You can configure an Event Rule triggered by a Folder Monitor Event to copy or move files in the folder and save them with a different name. Refer to Copy/Move File to Host Action for details of defining an Event Rule using the **Copy/Move file to host** Action.

IMPORTANT: If you want to move a modified (renamed) file, use the DST-based variables (for example, `%FS.DST_FILE_NAME%`) because they contain the modified values.

For example, when you configure an Event Rule to copy/move a file that is triggered on a **Monitor Folder** Event with a Condition of **If file change does equal to rename**, use the following variables:

- `%FS.DST_PATH%` instead of `%FS.PATH%`
- `%FS.DST_FILE_NAME%` instead of %`FS.FILE_NAME%`.

If the file is renamed, the new name context is lost to `FS.PATH` and `FS.FILE_NAME`, which retain the old path/name, but the new path/name is passed to `%FS.DST_PATH%` and `%FS.DST_FILE_NAME%`.

For example, suppose the monitored folder contained a file called `Robert.txt` and you rename the file `Bob.txt`.

`%FS.DST_FILE_NAME%` contains the new value `Bob.txt`, but `%FS.FILE_NAME%` contains the old value `Robert.txt`.

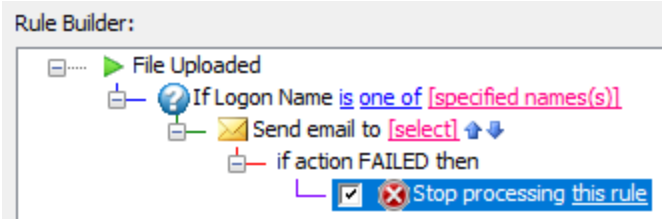
For details of the Copy/Move Action, refer to Copy or Move File to Host Action.

The client offload/download RENAME and the Folder Monitor RENAME are two different events/stimulus. The Folder Monitor RENAME uses the DST variables, whereas the client download/offload RENAME uses the SOURCE FILE NAME-related variables.

Example: Send an Email Notification When a Certain User Uploads a File

To send an email notification when a user or group of users uploads a file

1. Create an event rule using the event trigger **File Uploaded**.
2. Add the Condition **If Logon Name is** and specify the username. You can specify one or more user names. (For a group of users, you could use the **If User is a member of specific group**, such as Administrators or Guests.)
3. Add the Action **Protocol: Email** and add user variables such as %USER.LOGIN% and file system variables such as %FS.FILENAME%. (You could also use variables for the home folder, physical folder, virtual folder, home IP, and so on.)



Example: Copy/Move and Download File Cloud Storage Actions

The **Upload** and **Download file to cloud storage** Actions are used when you want to copy, move, or download files to/from Amazon S3 or Azure Blob storage. The **Cloud Connector Configuration** page in the Action wizard allows you so specify the cloud provider storage and other details, based on whether you specify Amazon S3 or Azure Blob storage.

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

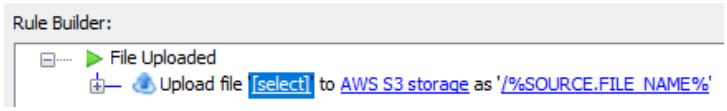
Be aware of the following AWS restrictions when creating a bucket name:

- Bucket names can contain lowercase letters, numbers, and hyphens.
- Each label must start and end with a lowercase letter or a number.
- A bucket name cannot start or end with a period.
- Bucket names must be at least 3 and no more than 63 characters long.
- Bucket names must not be formatted as an IP address (for example, 192.168.5.4).
- As a best practice, always use DNS-compliant bucket names regardless of the region in which you create the bucket. For example, MyAWSBucket is a valid bucket name, even though it contains uppercase letters. If you try to access this bucket by using a virtual-hosted–style request (http://MyAWSBucket.s3.amazonaws.com/yourobject), the URL resolves to the bucket myawsbucket and not the bucket MyAWSBucket. In response, Amazon S3 will return a "bucket not found" error.
- For more information regarding buckets restrictions, limitations, and naming, refer to http://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html.
- Cloud transfers are performed in multi-part sequential files. You can configure an advanced property to revert to legacy behavior (chunked transfers in parallel).

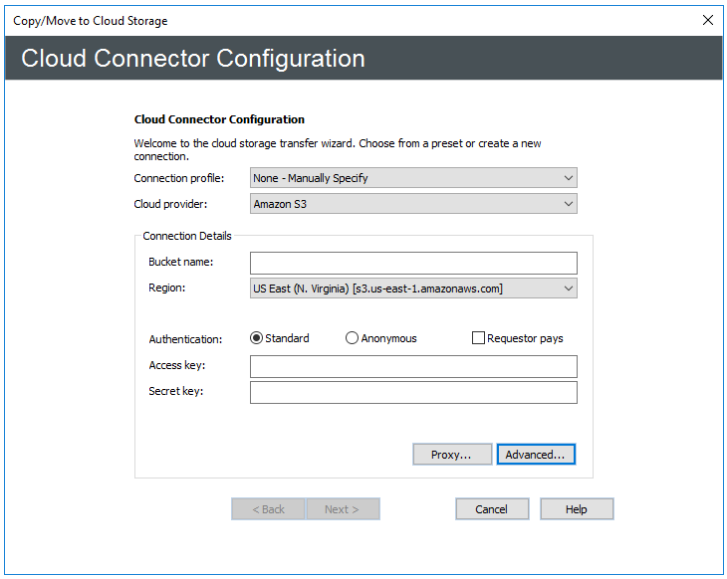
Refer to https://kb.globalscape.com/KnowledgebaseArticle11437.aspxfor details of the advanced property.

To configure Copy/Move and Download file to cloud storage Event Rules

1. After specifying an event in the Rule Builder, in the **Actions**list, double-click **Copy/Move (push) to** or **Download file from cloud storage**.



2. In the Action that was added to the Event Rule, click **select**. The **Cloud Connection Configuration** page appears.



3. Specify the connection details. You could also configure a cloud provider in a Connection profile to avoid having to configure connection details for every Event Rule.
4. Click **Advanced** to specify **Cloud Specific Transfer Options**. Refer to Specifying Advanced Transfer Options for configuration details.
    - **Can I use context variables?**

      Context variables are supported for passphrase and Metadata.

    - **What is the difference between Amazon S3 vs Amazon S3 (compatible)?**

      Amazon S3 (compatible) allows you to manually specify some of the fields (Endpoint URL, Region, host format). For example, for using with S3 compatible storage such as Google drive and others.

    - **Are the values in metadata passed as custom headers in the request to S3?**

      Metadata are passed as a custom header, with a name that starts with "x-

amz-meta-". For example:

```
x-amz-meta-metadatakey: MetadataValue
```

(For metadata details, refer to https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingMetadata.html.)

5. Click **Next**. In **Source File Path**, specify the source file. You can specify filenames, paths, or context variables.
6. Click **Next**. Specify the **Destination** for folder and filename (optional). Context variables can be used here also. Also in the **Destination**page of the wizard, you can specify what to do with matching filenames (Overwrite, Skip, or Numerate) and, can specify to rename the transferred file.
7. Click **Finish**.

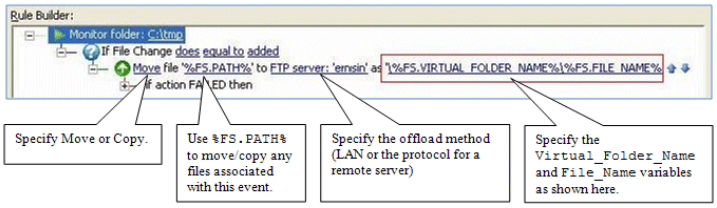
Refer to the following topics for information about creating EFT Event Rules:

- Introduction to Event Rules
- Defining a Connection Profile
- Defining Event Rules
- EFT Cloud Variables
- Cloud Object Monitor Event

Example: Copying Folder Structure When Offloading Files

In a **Monitor Folder** Event Rule, you can move a file that is added to the monitored folder. If you use the variables `%FS.VIRTUAL_FOLDER_NAME%\%FS.FILE_NAME%` as the Destination Folder path, the Event Rule will copy all of the files and folders and keep the folder structure. `VIRTUAL_FOLDER` contains the structure of the folders under the monitored folder.

The Event Rule in the illustration below will copy all of the files and keep their folder structure.



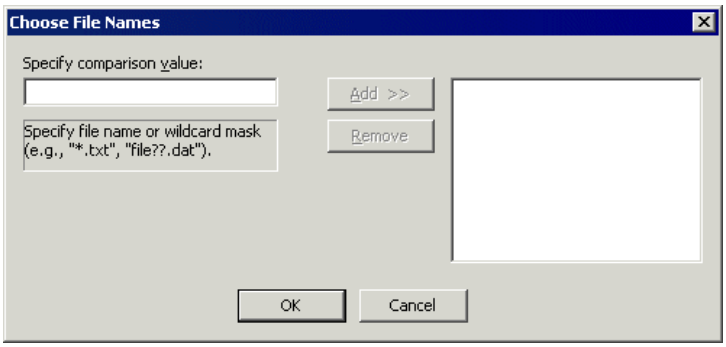
Refer to Monitoring Folders for details of creating a Folder Monitor Rule. Refer to Copy/Move (push) File to Host Action for details of using the **Copy/Move** Action.

Example: Moving an Uploaded File Based on Filename

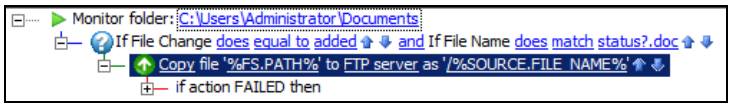
Suppose every Friday the manager of Engineering uploads a status report named `status<date>.doc` to EFT. You want the manager of Marketing to have access to that file, but not to any other files in the Engineering manager's folder. The example below describes how to create an Event Rule so that when a file with "status" in the name is uploaded to EFT, EFT makes a copy of it in another user's folder.

To move an uploaded file based on the filename

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, expand the Site you want to configure, and then click **Event Rules**. In the right pane, click **New**. The **Create New Event Rule** dialog box appears.
3. In the **Create New Rule** dialog box, click **Folder Monitor**, and then click **Create**. The new Rule appears in the **Rule Builder** and includes the **If File Change** Condition.
4. In the **Rule Builder**, in the Monitor folder Event, click **[select]**. The **Monitor Folder** dialog box appears.
5. Define the Monitor Folder trigger. If necessary, refer to Monitoring Folders for details of creating a Monitor Folder Rule. Note that if you create a Monitor Folder Rule to monitor a folder that is already being monitored by another Monitor Folder Rule, a warning message appears because the two Monitor Folder Rules can cause a race condition that may result in errors or undesirable results. If that is the case, you can add the new Conditions and Actions to the existing Rule.
6. Click the **If File Change** Condition in the **Rule Builder** to select it, then in the **Conditions** list, double-click the **If File Name** Condition. The **If File Name** Condition appears in the **Rule Builder** on the same line as the **If File Change** Condition. (See the screen shot in step 9 below.)
7. In the **If File Name** Condition, click the **[path mask]** link. The **Choose File Names** dialog box appears.



8. In the **Specify comparison value** box, specify the file name and/or a wildcard mask, click **Add**, and then click **OK**. For example, to filter for a Word document whose filename starts with "status, " type: `status?.doc`
9. Next, you must specify the Action to occur when this Event is triggered. In the right pane, in the **Actions** list, click **Protocol: Upload**. The Action is added to the **Rule Builder**.



10. Click one of the undefined parameters (for example, '%FS.PATH%'). The **Offload Action Wizard** appears.
11. In the **Offload method** box, specify a protocol type for the connection. For this example, we will choose **Local (Local Files or LAN)**. (Refer to ProtocolUploadAction for other protocol types.)
12. Click **Next**. The **Source File Path** page appears.
13. In the **Source path** box, type %FS.PATH% (or you can leave it blank).
14. If you want to **Delete source file after it has been offloaded**, select the check box. (If the file is marked read-only, it will not be deleted.)
15. Click **Next**. The **Destination File Path** page appears.
16. In the **Destination path** box, click the folder icon and specify the location in which to save the offloaded file. (No validation is performed.) In this example, we specified a user's folder.
17. Click **Finish** then click **Apply** to save the changes on EFT. (You could also add other Actions, such as email notifications.)

    Now when a user uploads a file called `status?.doc`, EFT will move it to the destination folder specified.

If you are copying or moving the file to another location, and the file upload is a regularly occurring Event with a file of the same name, in the **Offload Action** wizard, you can add the variables `%EVENT.DATESTAMP%` and/or `%EVENT.TIMESTAMP%` to the path so that the date (YYYYMMDD) and/or time (HHMMSS) are added to the filename when it is moved/copied.

> **WARNING:** Do ***not*** use `%EVENT.TIME%`, because the colon (for example, `28 Aug 07 10:01:56`) makes it invalid for file naming.

For example, type:

```
C:\Documents and Settings\administrator\My
Documents\upload\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%_%FS.FILE_
NAME%
```

With this path and variables, when a file is uploaded to the monitored folder, the file is moved to \My Documents\upload and the date and time are prepended to the filename (for example, 20080422_101212_mydailyprogress.doc).

Proxy Settings

The topics below describe how to define and use a proxy for event rules.

- Defining a Proxy
- Configuring Advanced Proxy Settings
- Using a SOCKS Proxy Server
- Routing Outbound Traffic through a Proxy

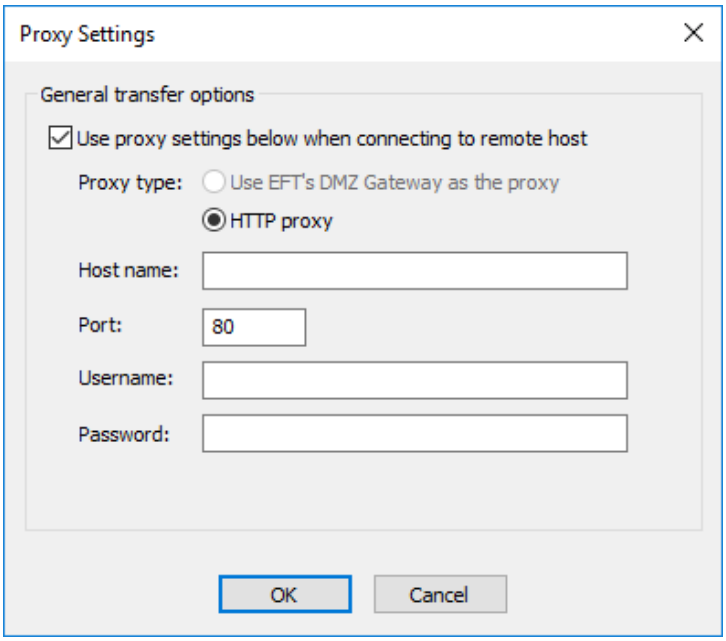
Defining a Proxy

If you connect to EFT through a proxy server, you must enable and define the proxy. The **Proxy Settings**dialog box appears in the Connection Profile, File Offload configuration (Copy/Move Action), File Download configuration (Download Action), and the Invoke Web Service from URL Actions.

- Using the DMZ Gateway as a proxy is not available when using Cloud Connection profiles. EFT uses the AWS SDK, which does not support the SOCKS protocol, which is required to proxy communications via the DMZ Gateway.
- Contact your system administrator for the proper host name, port, user name, password, and proxy type, as well as any required advanced authentication methods.

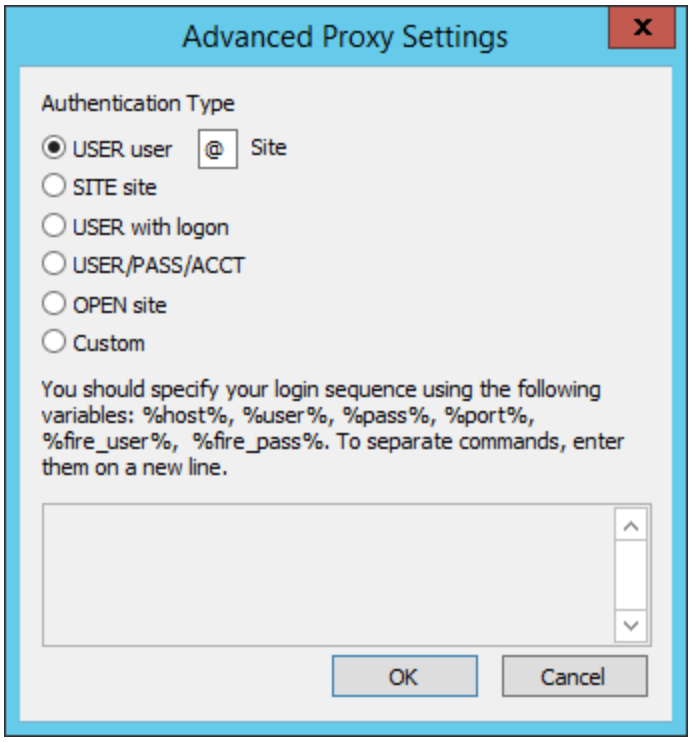
To configure the proxy settings

1. In the profile or action that you are configuring, click **Proxy**.
2. Select the **Use proxy settings**check box.
3. Specify the **Proxy type**.
4. Specify the **Host name**, **Port**, **Username**, and **Password** used to access the proxy server.



5. Click **Advanced** to specify an authentication type or login sequence. You must have selected **FTP Proxy** in the **Proxy Settings** dialog box to specify advanced

settings.


Advanced Proxy Settings
Authentication Type
USER user
@
Site
SITE site
USER with logon
USER/PASS/ACCT
OPEN site
Custom
You should specify your login sequence using the following variables: %host%, %user%, %pass%, %port%, %fire_user%, %fire_pass%. To separate commands, enter them on a new line.
OK
Cancel

Specify one of the following **Authentication Types**:

- **USER user@site**if your proxy server requires the USER command followed by your user name and the Site name to allow connection with a remote Site. You can change the @ symbol if a different separator is required by your proxy server.
- **SITE site**if your proxy server requires the SITE command followed by the address of the remote FTP site to allow a connection.
- **USER with logon**if your proxy server requires the USER command followed by a user name and password to allow connection with a remote Site.
- **USER/PASS/ACCT**if your proxy server requires all three commands before allowing a connection to a remote Site.
- **OPEN site**if your proxy server requires the OPEN command followed by the Site name before allowing connection to the Site.
- **Custom**if your proxy server requires a login sequence different from those above. Refer to the procedure below for details of creating a custom authentication method (login sequence).

  To create a custom authentication method for a proxy server

  i. In the **Advanced Proxy Settings** dialog box, click **Custom**, then specify the login sequence in the text box using the following variables: %host%, % user%, %pass%, %port%, %fire_pass%, %fire_ user%. Be sure to type each variable with percent signs before and after, and press ENTER to separate commands.

  ii. Type any other commands and variables, separating commands with a line break (press ENTER).

  iii. Click **OK**to accept the changes and close the **Advanced Proxy Settings** dialog box.

6. Click **OK** to accept the changes and close the **Advanced Proxy Settings** dialog box.
7. Click **OK** to accept the changes and close the **Proxy Settings**dialog box.

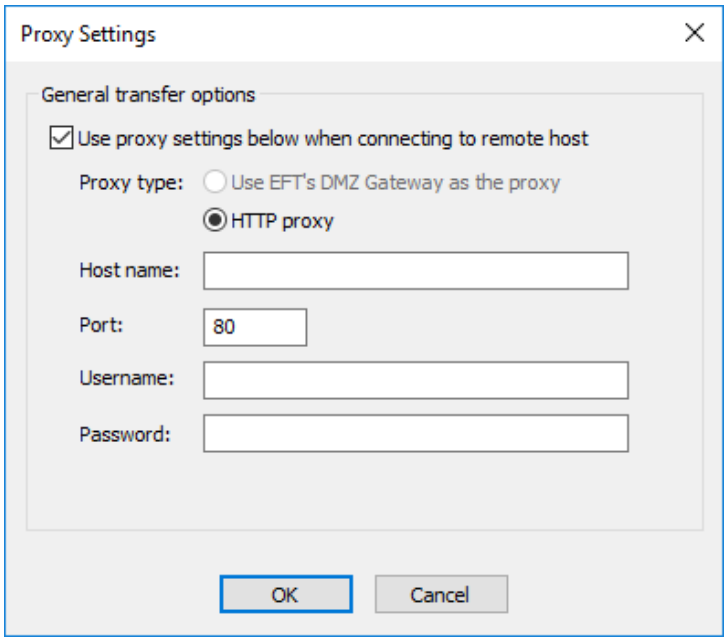
Configuring Advanced Proxy Settings

If you connect to EFT through a proxy server, you must enable and define the proxy. The **Advanced Proxy Settings**dialog box appears in the Connection Profile, File Offload configuration (Copy/Move Action), File Download configuration (Download Action), and the Invoke Web Service from URL Actions.

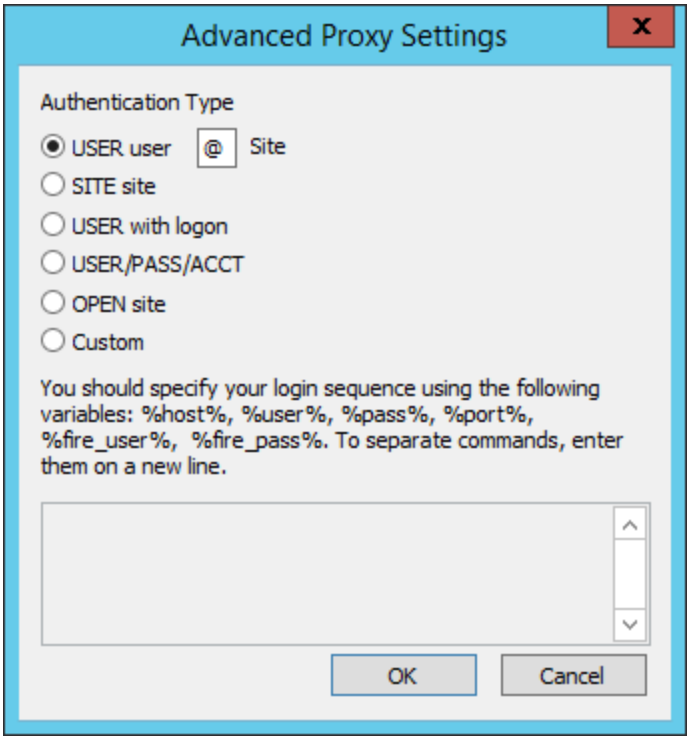
- Using the DMZ Gateway as a proxy is not available when using Cloud Connection profiles. EFT uses the AWS SDK, which does not support the SOCKS protocol, which is required to proxy communications via the DMZ Gateway.
- Contact your system administrator for the proper host name, port, user name, password, and proxy type, as well as any required advanced authentication methods.

To configure advanced proxy settings

1. In the profile or action that you are configuring, click **Proxy**.
2. Select the **Use proxy settings**check box.
3. Specify the **Proxy type**.
4. Specify the **Host name**, **Port**, **Username**, and **Password** used to access the proxy server.



5. Click **Advanced** to specify an authentication type or login sequence. You must have selected **FTP Proxy** in the **Proxy Settings** dialog box to specify advanced settings.



Specify one of the following **Authentication Types**:

- **USER user@site**if your proxy server requires the USER command followed by your user name and the Site name to allow connection with a remote Site. You can change the @ symbol if a different separator is required by your proxy server.
- **SITE site**if your proxy server requires the SITE command followed by the address of the remote FTP site to allow a connection.
- **USER with logon**if your proxy server requires the USER command followed by a user name and password to allow connection with a remote Site.
- **USER/PASS/ACCT**if your proxy server requires all three commands before allowing a connection to a remote Site.
- **OPEN site**if your proxy server requires the OPEN command followed by the Site name before allowing connection to the Site.
- **Custom**if your proxy server requires a login sequence different from those above. Refer to the procedure below for details of creating a custom authentication method (login sequence).

To create a custom authentication method for a proxy server

i. In the **Advanced Proxy Settings** dialog box, click **Custom**, then specify the login sequence in the text box using the following variables: %host%, % user%, %pass%, %port%, %fire_pass%, %fire_ user%. Be sure to type each variable with percent signs before and after, and press ENTER to separate commands.

ii. Type any other commands and variables, separating commands with a line break (press ENTER).

iii. Click **OK**to accept the changes and close the **Advanced Proxy Settings** dialog box.

6. Click **OK** to accept the changes and close the **Advanced Proxy Settings** dialog box.
7. Click **OK** to accept the changes and close the **Proxy Settings**dialog box.

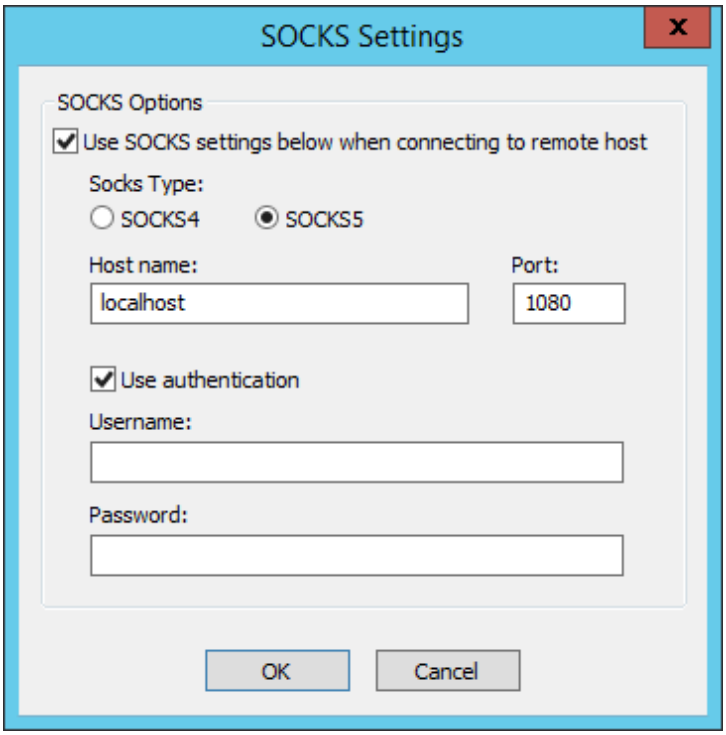
Using a SOCKS Proxy Server

When you create an Event Rule that requires the use of a SOCKS proxy server, you can specify settings in EFT for the connection to the SOCKS proxy server.

If you enable the use of DMZ Gateway as the proxy in the Proxy Settings dialog box, SOCKS options are disabled. EFT does not support the use of DMZ Gateway as a proxy and SOCKS settings in combination. For cloud connections, EFT uses the AWS SDK, which does not support the SOCKS protocol, which is required to proxy communications via the DMZ Gateway.

To use a SOCKS proxy server

1. Create an Event Rule.
2. In the Event Rule Action, click **%FS.PATH%**. The **Offload Action** wizard appears.
3. Click **Socks**. The **SOCKS Settings** dialog box appears.



4. Select the **Use SOCKS settings** check box to enable the **Socks Type**options.
5. In the **Socks Type**area, specify a SOCKS server type of either SOCKS4 or SOCKS5.

- When SOCKS4 is specified, **Use authentication** is disabled.
- When SOCKS 5 is specified, **Use authentication** can be enabled, allowing you to provide a username and password for the SOCKS connection. If you selected SOCKS5 and the **Use authentication** check box, specify the **Username**and **Password** required to connect to the SOCKS server.

6. Click **OK** to save the SOCKS options.

Routing Outbound Traffic through a Proxy

You can connect to EFT through an outbound proxy. DMZ Gateway can also be configured as an outbound proxy. There are several places in the administration interface in which you can configure proxy settings. Each of the configurations use the **Proxy Settings** dialog box.

Outbound connections that originate from EFT will route through normal network mechanisms to reach the destination. However, it is possible to configure Event Rules using the **Copy/Move file to host** Action to use a remote proxy.

To configure an Event Rule to route outbound traffic through a proxy

1. Create an Event Rule, such as a Scheduler (Timer) Event.
2. Add the **Copy/Move File to Host** Action, and follow the procedures in Copy/Move File to Host Action to complete the Rule.

For the procedure for using a SOCKS proxy server, refer to Using a SOCKS Proxy Server.

Related Topics

- Configuring an AS2 Outbound Proxy
- Using a SOCKS Proxy Server

EFT Variables

This section provides details of the EFT context variables. EFT uses *context variables* to pull data from the database. The variable contains specific information about an Event. You can use the variables in Event Rules, email notifications, and Advanced Workflows.

- How to Use EFT Context Variables
- Advanced Workflow Variables- Properties associated with Advanced Workflows, used when the Execute Advanced Workflow Action is added to an Event Rule.

  > **NOTE:** In the Advanced Workflows module, variables cannot contain periods; therefore, in each variable that contains a period, the period is replaced with an underscore. For example, change `%CONNECTION.LOCAL_IP%` to `%CONNECTION_LOCAL_IP%`

- AS2-Related Variables - Status of AS2 transfers (available only in AS2-related Event triggers)
- Cloud Variables - Used in the Download from Cloud Storage Action and Send Email Notification for Cloud Event Rules

  > **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

- Connection Variables - IP address, port, etc. for connecting to EFT
- Event Properties Variables - Name, date, time, reason, etc. for Event trigger
- File System Variables - File name, date, size, path, etc. that was transferred; also report name and content
- Remote Agent Variables- Properties associated with Remote Agent activities, such as Remote Agent template name, status, last update, and so on.
- Scheduler (Timer) Rule Variables - Used for Scheduler (Timer) Rules (For file operation triggers, use File System Variables.)
- Server Variables - Server status, logs, and computer name
- Site Variables - Site URL and status
- Transfer Properties Variables- Properties associated with the transfer: Speed, size, and seconds to transfer
- User Variables - User name, login information, etc.

- Workspaces-Related Variables- Virtual/physical path, owner, and so on.
- Using Context Variables for Parameterized Event Rules

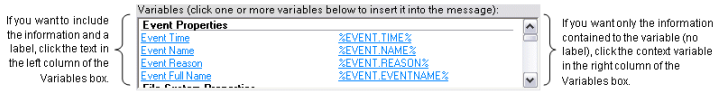
> **NOTE:** EFT can also use other variables as described in Context Variable Condition, Runtime Template Variables, Upload Forms, Flow: Variable Action, Flow: Subroutine Action, and Workspaces-Related Variables.

How to Use the Variables

In the **Variables** box, click a property that you want to insert.

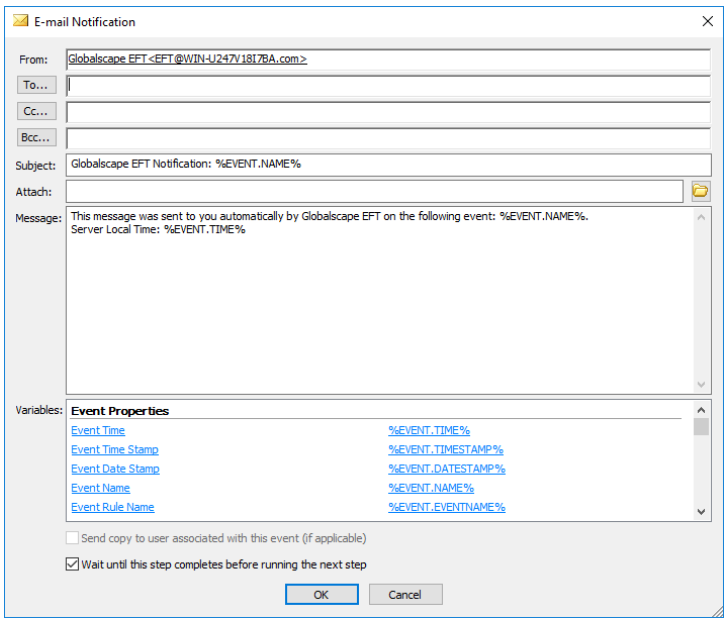
- If you just want the information contained to the variable, click the variable in the right column of the **Variables**box.
- If you want the information ***and***a label, click the text in the left column of the **Variables**box.

For example, if you click Event Time in the left column the label "Event Time" and the time are displayed. If you select `%EVENT.TIME%` in the right column, the time will be displayed without a text label.



For example, when you create an Event Rule, you can configure an email to be sent when the Event occurs. In the **Edit Mail Template** dialog box, you can send the default email or you can add one or more variables listed in the **Variables**box at the bottom of the email. Each of the variables defined in EFT is described in Connection Variables; however, not all of the variables described below are available in the email notification. In the email notification, you can specify to display the text along with the value of the variable (e.g., File Creation Date: 8/28/2022), or just the value of the variable (e.g., 8/28/2022).

Suppose you configured this email notification:



You then uploaded a file on August 28, 2007 at 10:01:56. The email would appear similar to the following:

```
This message was sent to you automatically by EFT on the
following Event: File Uploaded.

Event Time: 28 Aug 22 10:01:56

File Creation Date: 8/28/20202

File Creation Time: 10:01:56

Event Date Stamp: 20200828

Event Time Stamp: 100156
```

NOTE: In Event Rules and Commands with a defined path or file name, do not use variables that add invalid file name characters, such as a slash, colon, parenthesis, etc.

For example, you cannot use `%FS.FILE_CREATE_DATE%`and `%FS.FILE_CREATE_TIME%`for file naming, because the output of these variables is DD/MM/YYYY and HH:MM:SS and the forward slash (/) and colon (:) are not valid characters for filenames.

In most cases, the file created date and time is the same as the Event triggered time, therefore you can use `%EVENT.DATESTAMP%`(YYYYMMDD) and `%EVENT.TIMESTAMP%`(HHMMSS) when renaming files (because they do not use invalid characters), and `%FS.FILE_CREATE_DATE%`and `%FS.FILE_CREATE_TIME%`for email notifications.

For example, suppose an OnUpload Event Rule causes an Offload Action that moves myfile.txt to the following path:

```
C:/Inetpub/EFTRoot/Site1/Usr/jsmith/%EVENT.DATESTAMP%_%FS.FILE_NAME%
```

The resulting path is:

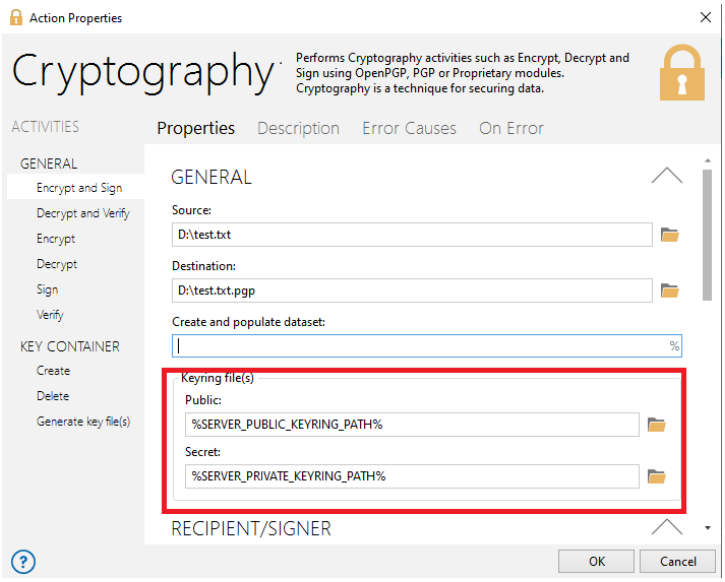
```
C:/Inetpub/EFTRoot/Site1/Usr/jsmith/20070728_myfile.txt
```

Advanced Workflow Variables

Used when the Execute Advanced Workflow Action is added to an Event Rule.

Text Displayed	Variable	Description
Advanced Workflow Name	%AWE.TASK_NAME%	Workflow name
Advanced Workflow Log Path	%AWE.LOG_PATH%	Workflow log path
Advanced Workflow Error Code	%AWE.ERROR_CODE%	Workflow error code
Advanced Workflow Error Description	%AWE.ERROR_DESCRIPTION%	Workflow error description
Advanced Workflow Error Line	%AWE.ERROR_LINE%	Workflow error line
Advanced Workflow Result Code	%AWE.RESULT_CODE%	Workflow result code displayed in the Windows Event Log and others
Advanced Workflow Result Description	%AWE.RESULT_DESCRIPTION%	Workflow result description displayed in the Windows Event Log and others
Advanced Workflow Execution Time (ms)	%AWE.EXECUTION_TIME_MS%	Workflow execution time (ms)

You can also pass other EFT variables into the Advanced Workflow Actions. For example, the path to the OpenPGP keyring files can be passed to the workflow with the %SERVER_PUBLIC_KEYRING_PATH% and %SERVER_PRIVATE_KEYRING_PATH% variables.



AS2 Variables

Status of AS2 transfers (**available only in AS2-related Event triggers**)

Text Displayed	Variable	Value Contained in Variable
AS2 Content Type	%AS2.CONTENT_TYPE%	Transfer's content type: Application, EDIFACT, XML, Mutually defined EDI, Binary, Plaintext
AS2 Direction	%AS2.DIRECTION%	Direction of the transfer
AS2 EFT ID	%AS2.EFT_ID%	EFT ID used in this transfer
AS2 Host	%AS2.HOST%	Address of the host being sent to (outbound) or received from (inbound)
AS2 Local MIC	%AS2.LOCAL_MIC%	Local AS2 message identification code (MIC)
AS2 MDN	%AS2.MDN%	Message Disposition Notification. The Internet messaging format used to convey a receipt.
AS2 Message ID	%AS2.MESSAGE_ID%	AS2 message identifier
AS2 Partner ID	%AS2.PARTNER_ID%	Transaction partner's AS2 ID
AS2 Payload	%AS2.PAYLOAD%	Name of the file (or an array of file names if MA is used) being transferred over the AS2 session
AS2 Remote MIC	%AS2.REMOTE_MIC%	Remote AS2 message identification code (MIC)
AS2 Transaction Error	%AS2.TRANSACTION_ERROR%	Error (if any) in the AS2 transaction
AS2 Transaction Result	%AS2.TRANSACTION_RESULT%	Overall transaction result (**In Progress**, **Failure**, or **Success**) of the in-context AS2 transaction
AS2 Transaction Verbose	%AS2.TRANSACTION_VERBOSE%	Verbose message for the AS2 transaction

Cloud Variables

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

Used in the **Download from Cloud Storage**Action and **Send Email Notification**for Cloud Event Rules

Text Displayed	Variable	Description
Cloud Object Content Length	%CLOUD.OBJ_META_CONTENT_LENGTH%	Object's size in bytes
Cloud Object Content MD5	%CLOUD.OBJ_META_CONTENT_MD5%	Base64-encoded 128-bitMD5 digest of the object
Cloud Object Date	%CLOUD.OBJ_META_DATE%	Object's date from meta data
Cloud Object Last Modified	%CLOUD.OBJ_META_LAST_MODIFIED%	Object's date last modified
Cloud Object Version ID	%CLOUD.OBJ_META_VERSION_ID%	From x-amz-version-id, which is the object version
Cloud Object Key Name	%CLOUD.OBJ_KEY_NAME%	Exact object name (e.g., 4my$-organization, or my.great_photos-2014/jan/myvacation.jpg
File Change	%CLOUD.MONITOR_OPERATION%	Operation of file change (create, delete, and rename)

Connection Variables

IP address, port, etc. for connecting to EFT

Text Displayed	Variable	Description
HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%	HTTP header string
HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%	HTTP header list
Local IP	%CONNECTION.LOCAL_IP%	Local IP address used to connect
Local Port	%CONNECTION.LOCAL_PORT%	Local port used to connect
Protocol	%CONNECTION.PROTOCOL%	Protocol used to connect
Remote IP	%CONNECTION.REMOTE_IP%	Remote IP address used to connect
Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%	Indicates whether the user connected via the Web Transfer client

Event Properties Variables

Name, date, time, reason, etc. for Event trigger

Text Displayed	Variable	Description
Event Date Stamp	%EVENT.DATESTAMP%	Date that the Event was triggered, e.g., `20070828` (suitable for file naming)
Event Rule Name	%EVENT.EVENTNAME%	User-defined name for the Event Rule (e.g., My File Renamed Event Rule)
Event Name	%EVENT.NAME%	Server-defined name for the Event trigger (e.g., File Renamed)
Event Reason	%EVENT.REASON%	Action completed successfully or Action Failed
Event Time	%EVENT.TIME%	Date and time that the Event was triggered, e.g., `28 Aug 07 10:01:56` (This variable is**not** suitable for file naming because of the colons; use %EVENT.DATESTAMP% and %EVENT.TIMESTAMP% when using variables for a filename.)
Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%	Time to the millisecond when Event was triggered (e.g., Event Time Stamp (including milliseconds): 154207233)
Event Time Stamp in ISO8601 format	%EVENT.DATE_TIME_ISO8601%	Date and time that the Event Was triggered in ISO8601 format: 2019-01-14T20:10:19Z 2019-01-14T20:10:19+0500
Event Timestamp	%EVENT.TIMESTAMP%	Time that the Event was triggered, e.g., `100156` (suitable for file naming)
Event Transaction ID **(EFT Enterprise only)**	%EVENT.TRANSACTION_ID%	The Transaction ID as logged by the database EFT is connected to (with ARM). This ID can be used to backtrack and find it in the database manually or to generate queries to the database.
Folder Monitor Failure Reason	%EVENT.MONITORFAILUREREASON%	Reason why the Folder Monitor Rule failed.

Text Displayed	Variable	Description
Folder Monitor Health	%EVENT.MONITORHEALTH%	Health of network share
Event Rule Failure Reason	%EVENT.ACTION_FAILURE_REASON%	Set to a string that represents the failure cause for event rule actions.

File System Variables

File name, date, size, path, etc. that was transferred; also report name and content

Text Displayed	Variable	Description
Report File	%FS.REPORT_FILE%	The full path of the report generated by the Generate Report Action, including the file name. This variable can be used in copy/move, OpenPGP, and custom commands that have a failure Event defined, but should not be used for custom command actions that do not have a failure Event defined.) In some cases, it may be more appropriate to use %FS.REPORT_CONTENT% because this variable represents a copy of the contents of the file rather than a link to the file, which is only good so long as the file exists. For example, since the file will be deleted when EFT stops processing the Event Rule, **do not use this variable in email notifications**; use %FS.REPORT_CONTENT% instead.
Report Content	%FS.REPORT_CONTENT%	Contents of the report generated by the Generate Report Action. This variable is typically used after creation of an HTML report, in an email notification action, where it is desirable to embed the HTML contents of the report as the email body.
Report File Name	%FS.REPORT_FILENAME%	The name of a report file created by a Generate Report action. This variable is typically used after creation of a PDF report file, in an email notification, to provide the destination path for the report file after a Copy/Move action deposits it in a more permanent location.
Virtual Path	%FS.VIRTUAL_PATH%	Virtual location of the file (See a list of uses for this variable below.)
Physical Path	%FS.PATH%	Physical location of the file
File Change	%FS.MONITOR_OPERATION%	File change that triggered the Event (added, removed, etc.) Used in Folder Monitor rules
Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%	The structure of the virtual folders
Physical Folder Name	%FS.FOLDER_NAME%	Name of the physical folder
Virtual Directory Name	%FS.VIRTUAL_DIR_NAME%	Name of virtual directory, without the whole path
Base File Name	%FS.BASE_FILE_NAME%	Name of the file without the extension

Text Displayed	Variable	Description
File Extension	%FS.FILE_EXTENSION%	File extension; Takes anything after the last dot (before the extension) and places it into this context variable. (e.g., for `document.docx`, `docx`is the value of the variable.) This variable can be used anywhere %FS.BASE_FILE_NAME% can be used.
File Name	%FS.FILE_NAME%	Name of the file with the extension
File Size	%FS.FILE_SIZE%	Size of the file involved in the Event
File CRC	%FS.FILE_CRC%	This variable is only applicable for "Verify Uploaded" events using HTTP and HTTPS protocols.
File Creation Date	%FS.FILE_CREATE_DATE%	Date the file was created, in the format YYYY/MM/DD, e.g., `8/28/2007`(**not** suitable for file naming because of the slashes)
File Creation Time	%FS.FILE_CREATE_TIME%	Time the file was created, in the format HH:MM:SS, e.g., `10:01:56`(**not** suitable for file naming because of the colons)
File Creation Date in ISO8601 format	%FS.FILE_CREATION_DATETIME_ISO8601%	File Creation Date in ISO8601 format 2019-01-14T20:10:19Z 2019-01-14T20:10:19+0500
File Modification Date in ISO8601 format	%FS.FILE_MODIFICATION_DATETIME_ISO8601%	File Modification Date in ISO8601 format 2019-01-14T20:10:19Z 2019-01-14T20:10:19+0500
Virtual Destination Path	%FS.DST_VIRTUAL_PATH%	Virtual destination path of the file involved in the Event
Physical Destination Path	%FS.DST_PATH%	Physical destination path of the file
Physical Destination Folder Name	%FS.DST_FOLDER_NAME%	Physical destination folder
Destination File Name	%FS.DST_FILE_NAME%	Destination file name
Compressed File Physical Path	%FS.COMPRESSED_PATH%	Physical path to the compressed file
Compressed File Name	%FS.COMPRESSED_FILE_NAME%	Name of the compressed file with the extension

Text Displayed	Variable	Description
Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%	Name of the compressed file without the extension

The following Event Rule Actions with paths can support the virtual path context variable (%FS.VIRTUAL_PATH%):

- Protocol: Upload
  - Source path
- Protocol: Download
  - Destination path
  - Rename transferred file to
- Protocol: Synchronize
  - Mirror local - Source path
  - Mirror remote - Destination path
- Protocol: AS2
  - File(s) to upload
- Protocol: Email
  - Attach
- Cloud: Upload
  - Source path
- Cloud: Download
  - Destination path
  - Rename transferred file to
- Cloud: Rest/Web Services
  - Save response to - File
- Compression
  - Source Path
  - Destination Path
- Cryptography: OpenPGP
  - File to process
- File: Scan
  - File Path

- File: Operation
    - Write operation - Destination Path
    - Read operation - Source Path
    - Rename operation - Source Path, Destination Path
    - Delete operation - Source Path
    - Concatenate operation - Source Path A, Source Path B, Destination Path
    - Checksum operation - Source Path
- Folder: Operation
    - Create action - Path (Destination of the path to be created)
    - Rename action - Path (Source Path), New Path (Destination Path)
    - Delete action - Path (Source Path)
- Script: Advanced Workflow
    - [Paths from custom parameters list] (Name/Value)

Remote Agent Context Variables

The Remote Agent Context Variables can be used in RAM Event Rules. Each of the variables is described below.

Text Displayed	Variable	Description
Remote Agent Name	%AGENT.NAME%	Computer name of remote system running the Remote Agent, enumerated if there is more than one Agent with that name.
Remote Agent Version	%AGENT.VERSION%	Version of Remote Agent update
Remote Agent Last Update Time Stamp	%AGENT.LAST_ UPDATE_TIMESTAMP%	Date of last Remote Agent update
Remote Agent Next Update Time Stamp	%AGENT.NEXT_ UPDATE_TIMESTAMP%	Date of next scheduled Remote Agent update
Remote Agent NetBIOS Name	%AGENT.COMPUTER_ NAME%	Computer name of remote system running the agent
Remote Agent Template	%AGENT.TEMPLATE%	Template name associated with the Agent
Remote Agent Status	%AGENT.STATUS%	Status of Remote Agent (e.g., Active, Pending, Approved, Denied, Banned)

Scheduler (Timer) Rule Variables

The %SOURCE.FILE_NAME% variable is available in the list box of **Destination Folder** page of the **Copy/Move** Action and **Download**Action wizards if the Rule is a Timer/Scheduler Rule.

- If the Rule has a file operation as a trigger (Folder Monitor, On File Upload, File Renamed by Connected Client, etc.) then the variable selection list will include the %FS.*% family of variables and they will have a valid value.
- If the Rule does not have a file operation as a trigger (Timer, User Connected, etc.) then the variable selection list will include the %SOURCE.*% family of variables.

If one of these non-file-trigger Rules contains an %FS.FILE_NAME% variable, it will be converted to %SOURCE.FILE_NAME% and a WARNING will record the change in the EFT.log.

The %SOURCE.FILE_NAME% and %SOURCE.BASE_FILE_NAME% can be used in a Timer Rule to download a mask of files (e.g., *.xml), and then FTP offload each of those files to a remote server with a *.TMP extension (%SOURCE.BASE_FILE_NAME%.TMP). After each file transfer is complete, you can then rename each individual file back to its original name (%SOURCE.FILE_NAME%).

Variable	Description
%SOURCE.BASE_FILE_NAME%	Source file name without extension
%SOURCE.FILE_NAME%	Source file name with extension

Server Variables

Server status, logs, and computer name

Text Displayed	Variable	Description
Log Location	%SERVER.LOG_LOCATION%	Location of the log file
New Log File Name	%SERVER.LOG_NEW_NAME%	New name of the log file
New Log File Path	%SERVER.LOG_NEW_PATH%	New path of the log file
Old Log File Name	%SERVER.LOG_OLD_NAME%	Old name of the log file
Old Log File Path	%SERVER.LOG_OLD_PATH%	Old path of the log file
Log Type	%SERVER.LOG_TYPE%	Either Standard or Verbose, per the setting on the **Logs** Tab
Node Name	%SERVER.NODE_NAME%	Computer name on which EFT is running
Server Running	%SERVER.STATUS%	Indicates whether the EFT service was running when the Event was triggered. (Yes or No)
Private Key ring path	%SERVER_PRIVATE_KEYRING_PATH%	Pass the location of the private key ring to the Advanced Workflows module
Public Key ring path	%SERVER_PUBLIC_KEYRING_PATH%	Pass the location of the private key ring to the Advanced Workflows module
Install Directory	%SERVER.INSTALL_DIRECTORY%	Directory in which the server is installed

Site Variables

Site URL and status

Text Displayed	Variable	Description
Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%	Site account management URL, **https://../manageaccount:<port>**(if port is not equal to 443)
Site Name	%SITE.NAME%	Site name
Site Running	%SITE.STATUS%	Indicates whether the Site was running when the Event was triggered. (Yes or No)
Data Protection Officer email	%SITE.PRIVACY_DPO_EMAIL%	Displays the email of the Data Protection Officer (DPO) that you specify in the GDPR dialog boxon the Site > Web tab.
DMZ Gateway Address	%SITE.DMZ_ADDRESS%	Displays the IP address of the DMZ Gateway
DMZ Gateway Port	%SITE.DMZ_PORT%	Displays the port of the DMZ Gateway

Transfer Properties Variables

Properties associated with the transfer: Speed, size, and seconds to transfer

Text Displayed	Variable	Value Contained in Variable
Transfer Rate	%TRANSFER.RATE_ KBPS%	Average speed of transfer (total bytes transferred/total seconds to transfer) Displayed in kilobytes per second (KBps).
Transferred Bytes	%TRANSFER.BYTES%	Total number of bytes in the transfer. **NOTE**: By default FTP uses built-in compression (MODE Z); therefore, it is possible for transferred bytes to be less than the file size. Moreover, the values for FTPS, SFTP, and HTTP could differ from file size due to internal compression and protocol overheads.
Transfer Seconds	%TRANSFER.SECONDS%	Total number of seconds it took to transfer

User Variables

User name, login information, etc.

Text Displayed	Variable	Description
Using Remote Agent	%USER.AGENT%	Indicates whether the user is using a Remote Agent (Yes or No)
User can connect using FTP	%USER.ALLOW_FTP%	Indicates whether user is allowed to connect using FTP (Yes or No)
User can connect using SFTP	%USER.ALLOW_SFTP%	Indicates whether user is allowed to connect using SFTP (Yes or No)
User can connect using SSL	%USER.ALLOW_SSL%	Indicates whether user is allowed to connect using SSL (Yes or No)
User can change password	%USER.CAN_CHANGE_PASSWORD%	Indicates whether the user is allowed to change the login password (Yes or No)
Comment	%USER_COMMENT%	Text in the **Comment**box, if defined in the **User Account Details** dialog box
Custom 1	%USER.CUSTOM1%	Text in the **Custom 1** box, if defined in the **User Account Details** dialog box
Custom 2	%USER.CUSTOM2%	Text in the **Custom 2** box, if defined in the **User Account Details** dialog box
Custom 3	%USER.CUSTOM3%	Text in the **Custom 3** box, if defined in the **User Account Details** dialog box
Description	%USER.DESCRIPTION%	Description of the user account, as defined on the **General** tab
DUNS Number	%USER.DUNS%	A user's organization's "DUNS number"; (The Data Universal Numbering System, DUNS, is a proprietary system developed and regulated by Dun & Bradstreet that assigns a unique numeric identifier to a single business entity.)
email Address	%USER.EMAIL%	email address of the user, if defined in the **User Account Details**dialog box. You can pass multiple addresses to the Advanced Workflow Engine using this variable.

Text Displayed	Variable	Description
Account Enabled	%USER.ENABLED%	User account is enabled:(Yes or No
Account Expiration Date	%USER.EXPIRATION_DATE%	Date in the default system locale when user account expired: Date , or `Never`
Account Expiration Date in ISO8601 format	%USER.EXPIRATION_DATETIME_ISO8601%	Displays the account expiration date in ISO8601 format 2019-01-14T20:10:19Z 2019-01-14T20:10:19+0500
(GDPR) User EU data subject status	%USER.EU_DATA_SUBJECT_STATUS%	User is an EU data subject: Yes, No, or Unknown
Fax Number	%USER.FAX%	Fax number of the user, if defined in the **User Account Details** dialog box
Full Name	%USER.FULL_NAME%	Full name of the user, if defined on the **User Account Details** dialog box
(GDPR) Reason given	%USER.GDPR_REASON_Given%	Reason the user exercised privacy rights (used with "Right exercised" variable)
(GDPR) Right exercised	%USER.GDPR_RIGHT_EXERCISED%	User has exercised the "right to be forgotten": Yes, No, or Unknown
(GDPR) Right exercised per Article ID	%USER.GDPR_RIGHT_EXCERCISED_ ARTICLE_ID%	Article ID is applicable to the right exercised by the user (used with "Right exercised" variable)
Groups	%USER.GROUPS%	Lists groups of which the user is a member
Home Folder	%USER.HOME_FOLDER%	User's home folder, for example, \asmith
Home Folder	%USER.HOME_FOLDER_PATH%	Entire path to a user's home folder (for example, C:\InetPub\EFTRoot\MySite\Usr\asmith)
Home IP	%USER.HOME_IP%	IP address of the user
Home Folder is Root	%USER.HOME_IS_ROOT%	**Treat Home Folder as Root** check box is selected: Yes or No

Text Displayed	Variable	Description
Invalid login attempts	%USER.INVALID_LOGINS%	Number of invalid login attempts by the user
User is locked out	%USER.IS_LOCKED_OUT%	Indicates whether user account is locked
Last Login Date	%USER.LAST_LOGIN%	Provides the date and time (in the default system locale) the user last logged in to EFT
Logon Name	%USER.LOGIN%	Login username of the user
Pager Number	%USER.PAGER%	Pager number of the user, if defined in the **User Account Details**dialog box
Logon Password	%USER.PASSWORD%	Login password of the user
Password Expiration Date	%USER.PASSWORD_EXPIRATION%	Provides date/time in the default system locale when the user account is set to expire, or `Never`
Password Expiration Date in ISO8601 format	%USER.PASSWORD_EXPIRATION_DATETIME_ISO8601%	Password Expiration Date in ISO8601 format 2019-01-14T20:10:19Z 2019-01-14T20:10:19+0500
Phone Number	%USER.PHONE%	Phone number of the user, if defined in the **User Account Details**dialog box
Consent status	%USER.PP_CONSENT_STATUS%	Returns the status of the Privacy Policy: Unknown, Granted (implicit), Granted (explicit), Denied, Rescinded
(GDPR) User consent to privacy policy	%USER.PP_CONSENT_STATUS%	User consented to the privacy policy: Unknown, Agreed (implicit), Agreed (explicit), Disagreed, or Withdrawn.
Quota Max	%USER.QUOTA_MAX%	Max disk space specified for the user
Quota Used	%USER.QUOTE_USED%	Amount of disk space in use by the user
User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%	Indicates whether user is required to reset the account password at first log in (Yes or No).
Settings Template	%USER.SETTINGS_LEVEL%	Settings Template of the user

Text Displayed	Variable	Description
(GDPR) User agreement to terms of service	%USER.TOS_AGREEMENT_STATUS%	User agreed to the terms of service: Unknown, Agreed (implicit), Agreed (explicit), Disagreed, or Withdrawn.

Workspaces-Related Variables

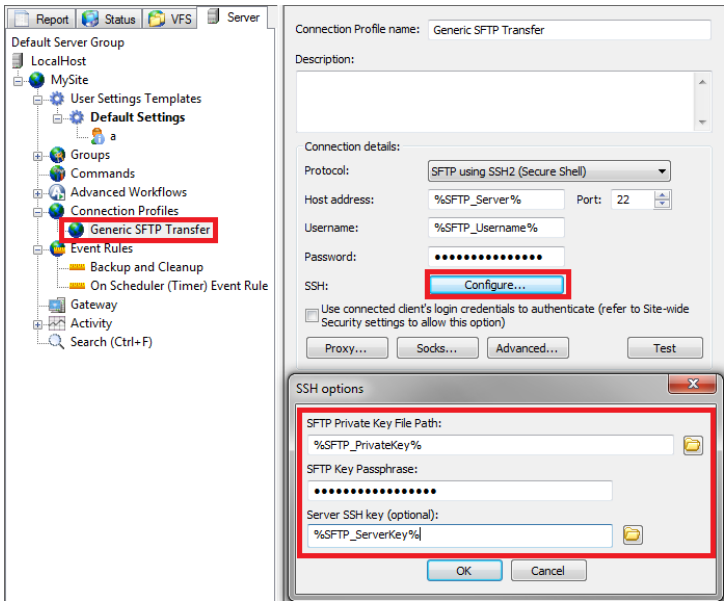
The variables below are for use in Event Rules for virtual/physical path, owner, and so on. The Workspaces notifications use different variables than these, as shown below.

Text Displayed	Variable	Value Contained in Variable
Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%	Virtual path of the Workspace
Workspace Physical Path	%WORKSPACE.PATH%	Physical path of the Workspace
Workspace Name	%WORKSPACE.NAME%	Name of the Workspace Folder
Workspace Participants List	%WORKSPACE.PARTICIPANTS%	Participants sharing the Workspace
Workspace Subject	%WORKSPACE.SUBJECT%	Subject line of the email sent via Workspaces
Workspace Message	%WORKSPACE.MESSAGE%	Message sent via Workspaces
Workspace Owner	%WORKSPACE.OWNER%	Owner of the Workspace
Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%	Email address of the owner of the Workspace; the variable is case sensitive when used in the To, Cc, or Bcc fields of email notifications.
Workspace User	%WORKSPACE.USER_NAME%	Username of the Workspace participant
Workspace User Permissions	%WORKSPACE.USER_ PERMISSIONS%	User permissions of the Workspace
Workspace User Email Address	%WORKSPACE.USER_EMAIL%	User email of the participant
Workspace User Account Exists	%WORKSPACE.USER_ACCOUNT_ EXISTS%	Identifies whether the user account exists (or needs to be created)

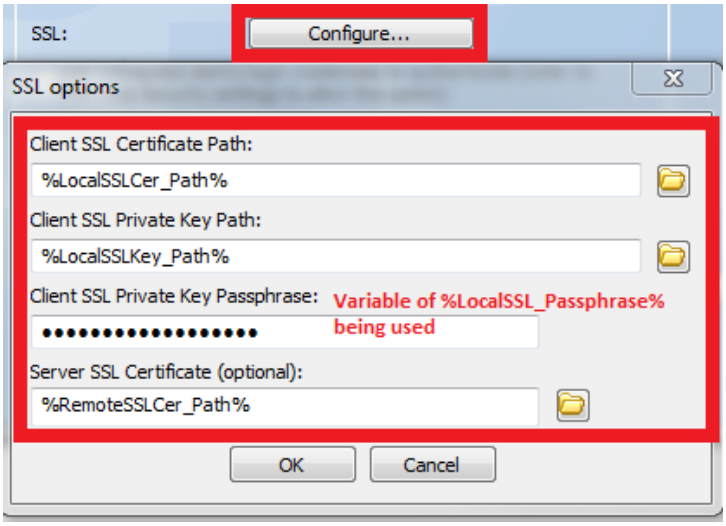
Using Context Variables for Parameterized Event Rules

Some EFT administrators have a need for "parameterized" event rules to do SFTP and FTPS transfers. When defining a Connection Profile or a connection directly within a Protocol: Upload Action or Protocol: Download Action, the administrator can use arbitrary Context (%...%) variables in the following dialog box fields:

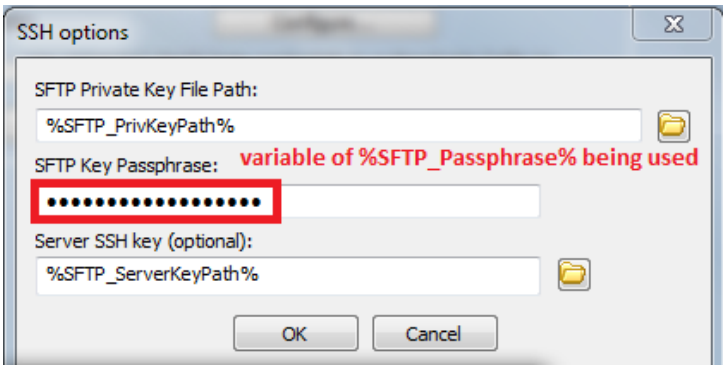
- SFTP Private Key Path
- SFTP Key Passphrase
- Server SSH Key
- Client SSL Certificate Path
- Client SSL Private Key Path
- Client SSL Private Key Passphrase
- Server SSL Certificate
- Connection Profile (SFTP and FTPS/HTTPS):



- Client SSL Certificate/Key/Passphrase Path and Server SSL Certificate Path:



- SFTP Private Key File Path/Passphrase/Key and Server SSH Key Path:



Events (Triggers)

The topics below provide examples of some common uses of Event Rules.

- Event Triggers
- AS2 Events
- Cloud Object Monitor Event
- Connection Events
- Event Rule Subroutine Event
- File Server Events
- File Uploaded Event
- Folder Monitor Event
- GDPR Right Exercised
- IP Added to Ban List
- Operating System Events
- REST Invocation Event
- Scheduler (Timer) Event
- Secure File Send Events
- Server Events
- Site Events
- User Events
- Workspaces Events
- Too Many Connections per Site
- Changing the Number of Concurrent Threads Used by Event Rules
- Applying a Rule to a Specific User or Group

Event Triggers

EFT includes more than 25 different event triggers, based on the following event types:

- Operating System-related events, such as a folder's contents changed or a recurring Timer has executed
- Cloud object monitor is similar to Folder Monitor, but is used to monitor folders in your cloud storage

  > **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

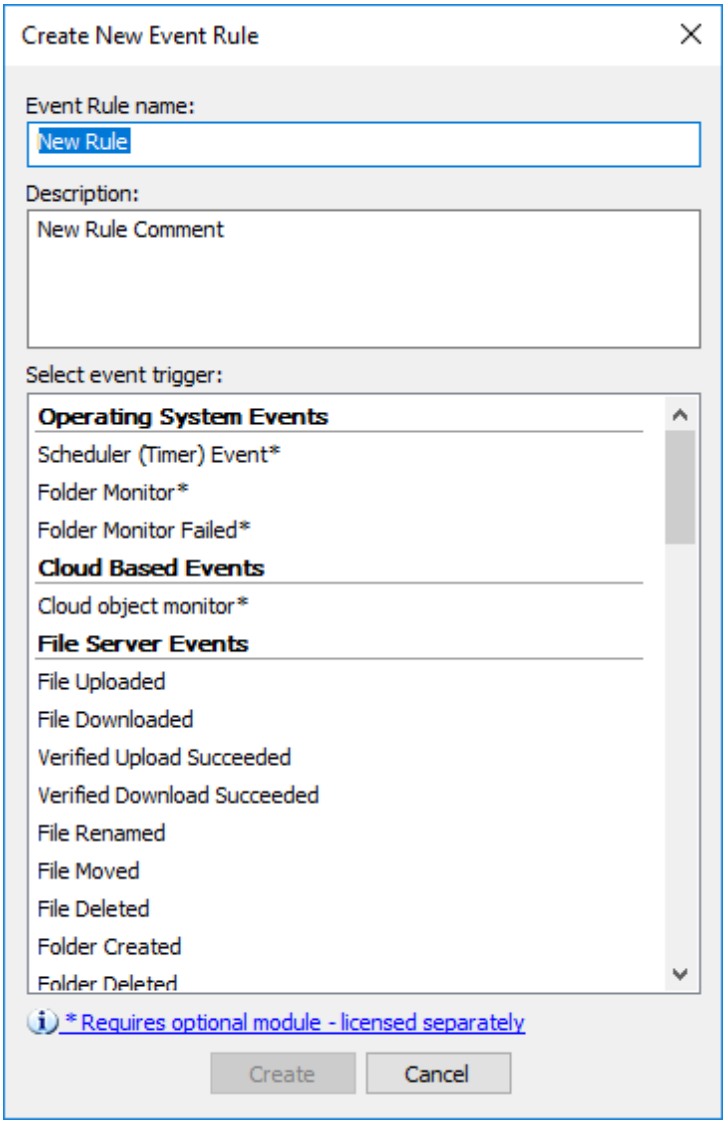
- File server-related events, such as file uploaded or file deleted
- Workspaces-related events, such as User Invited
- Secure File Send events, such as Message Not Sent
- Server-related events, such as Server stopped or started
- Site-related events, such as Site stopped or started
- User-related events, such as User Account Locked
- Connection-related events, such as a user connections failed
- AS2-related events, such as the transfer was successfully completed
- Event Rule Subroutine - The **Event Rule Subroutine** event is used to call another rule from the current rule to create more modular "functional" style of rules. With the **Event Rule Subroutine** event, you can build an event rule that calls a Call Event Rule Subroutine Action asynchronously, thus letting the target rule handle the burden of processing, while returning a reply immediately to the client.
- REST Invocation- The REST Invocation event is used to call up a specific REST endpoint, such as a remote webhook, or for non-administrative users to execute an event rule for inbound traffic.

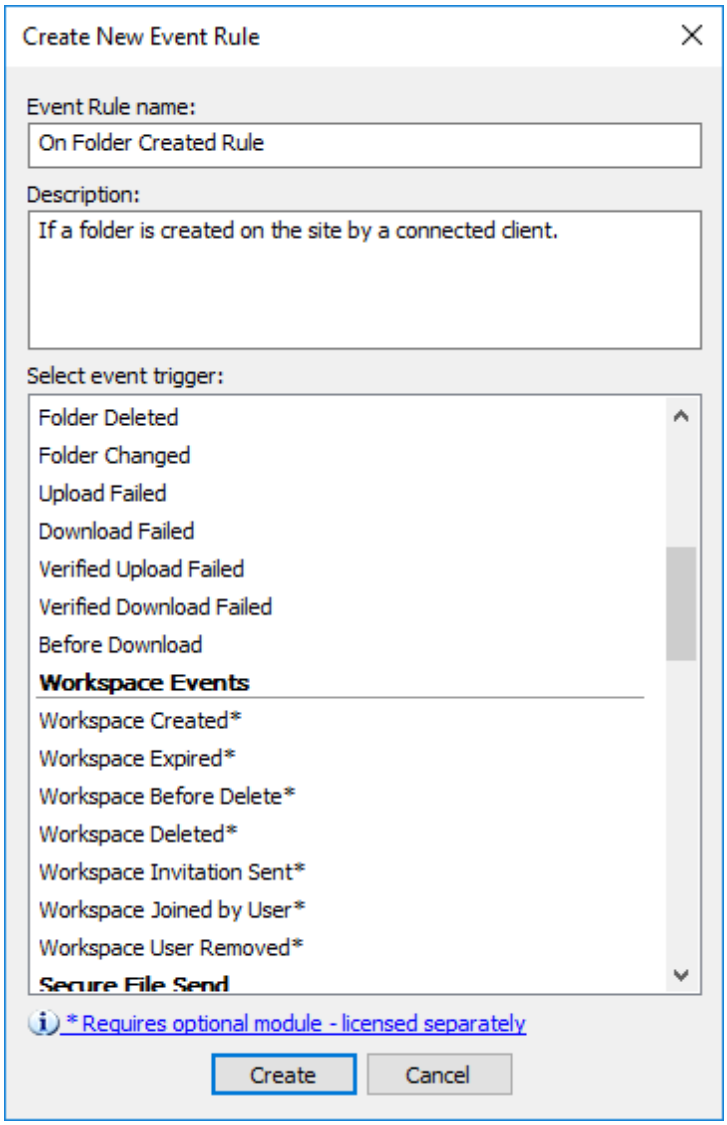
Not all variables are available with every Event trigger. For example, it does not make sense to use the %EVENT.REASON% variable with a File Downloaded Event, but it does make sense with the Upload Failed Event, because EFT can determine the reason for the failure.

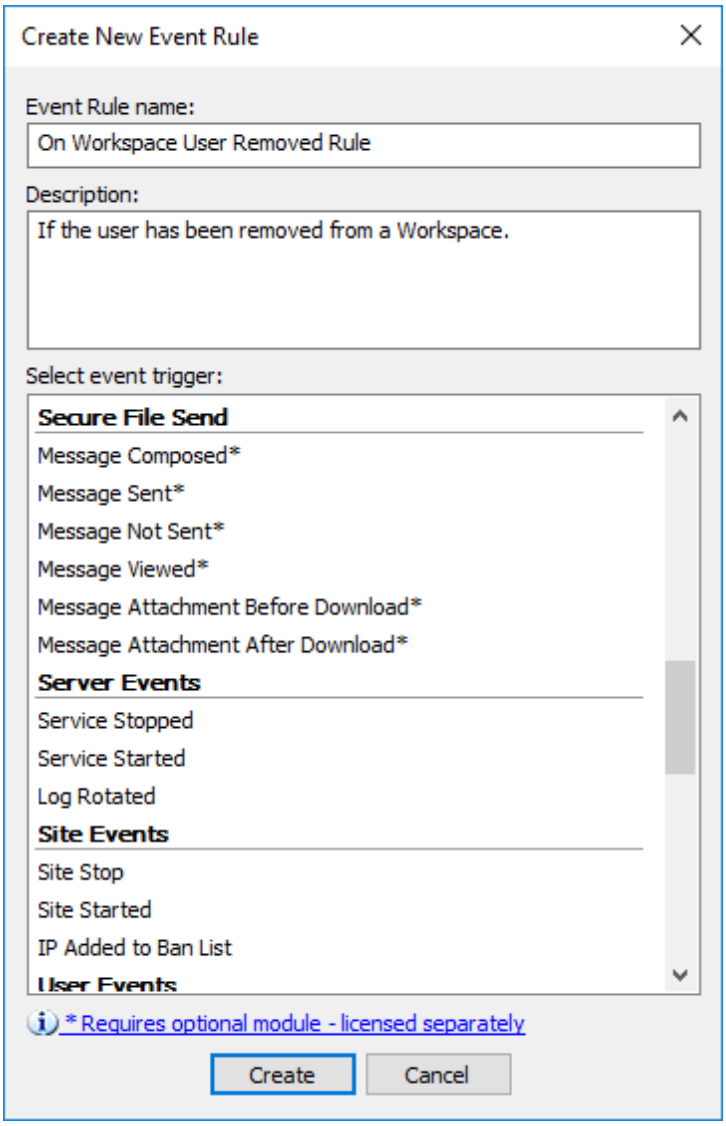
Refer to Variables for a description of each variable and caveats (for example, %EVENT.TIME% is not suitable for file naming and %FS.REPORT_FILE% should not be used in email notifications).

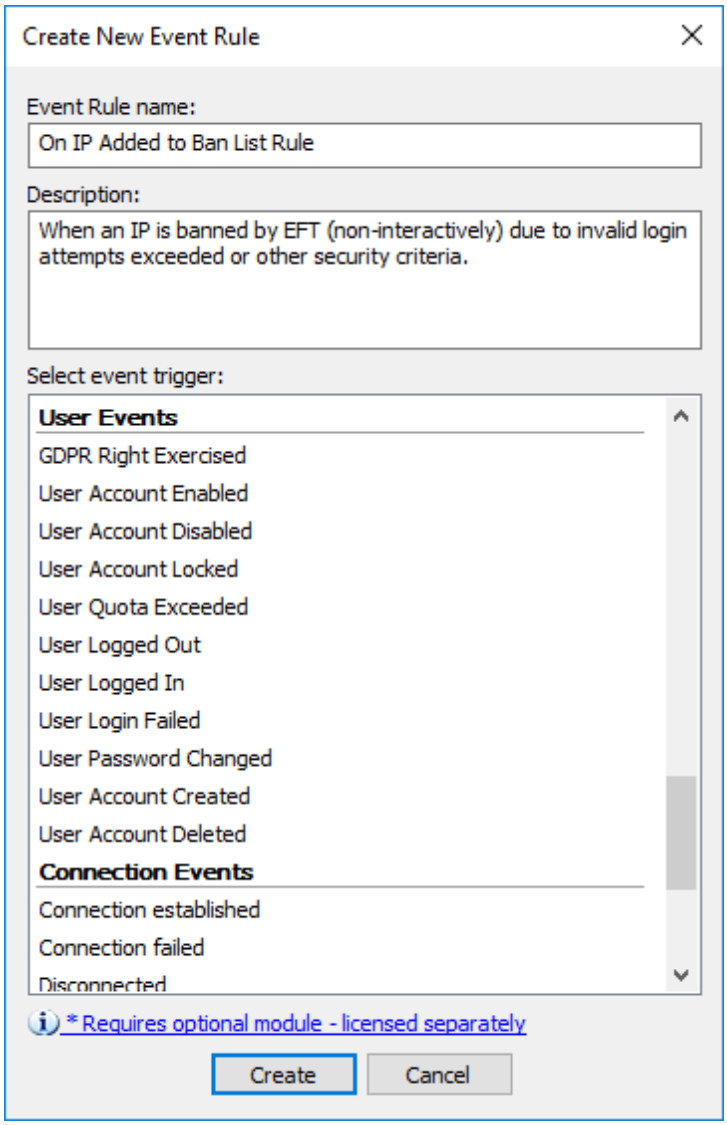
Refer to Which Actions can be Added to which Events for details of added Actions to Events.

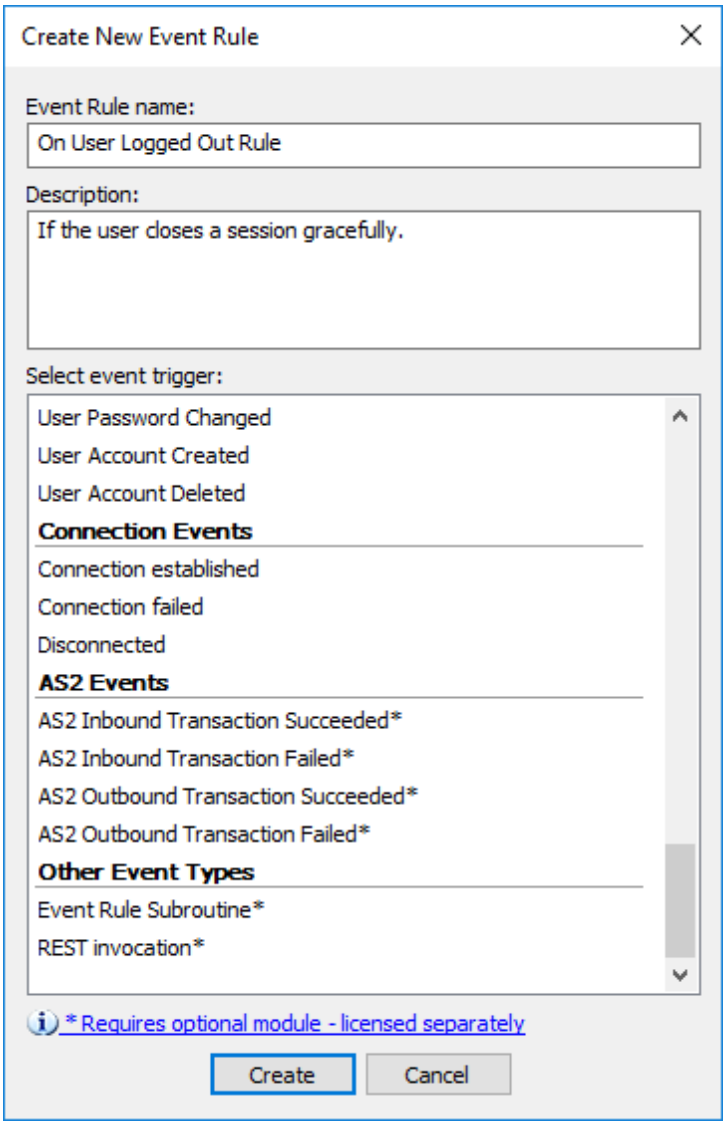
> **NOTE:** Event triggers marked with an asterisk in the **Create New Event Rule** dialog box require a module license. (See below.)




Create New Event Rule
Event Rule name:
On Folder Created Rule
Description:
If a folder is created on the site by a connected client.
Select event trigger:
Folder Deleted
Folder Changed
Upload Failed
Download Failed
Verified Upload Failed
Verified Download Failed
Before Download
Workspace Events
Workspace Created*
Workspace Expired*
Workspace Before Delete*
Workspace Deleted*
Workspace Invitation Sent*
Workspace Joined by User*
Workspace User Removed*
Secure File Send
* Requires optional module - licensed separately
Create
Cancel


Create New Event Rule
Event Rule name:
On Workspace User Removed Rule
Description:
If the user has been removed from a Workspace.
Select event trigger:
Secure File Send
Message Composed*
Message Sent*
Message Not Sent*
Message Viewed*
Message Attachment Before Download*
Message Attachment After Download*
Server Events
Service Stopped
Service Started
Log Rotated
Site Events
Site Stop
Site Started
IP Added to Ban List
User Events
* Requires optional module - licensed separately
Create
Cancel


Create New Event Rule
Event Rule name:
On IP Added to Ban List Rule
Description:
When an IP is banned by EFT (non-interactively) due to invalid login attempts exceeded or other security criteria.
Select event trigger:
User Events
GDPR Right Exercised
User Account Enabled
User Account Disabled
User Account Locked
User Quota Exceeded
User Logged Out
User Logged In
User Login Failed
User Password Changed
User Account Created
User Account Deleted
Connection Events
Connection established
Connection failed
Disconnected
* Requires optional module - licensed separately
Create
Cancel


Create New Event Rule
Event Rule name:
On User Logged Out Rule
Description:
If the user closes a session gracefully.
Select event trigger:
User Password Changed
User Account Created
User Account Deleted
Connection Events
Connection established
Connection failed
Disconnected
AS2 Events
AS2 Inbound Transaction Succeeded*
AS2 Inbound Transaction Failed*
AS2 Outbound Transaction Succeeded*
AS2 Outbound Transaction Failed*
Other Event Types
Event Rule Subroutine*
REST invocation*
* Requires optional module - licensed separately
Create
Cancel

AS2 Events

(Requires AS2 and ARM) In **AS2 Inbound Transaction Succeeded** and **AS2 Inbound Transaction Failed** Events, the `FS.FILE_NAME` variable contains the name of the file uploaded (for a simple transaction) or an empty string (for a Multiple Attachment (MA) transaction).

- **AS2 Inbound Transaction Succeeded**—Triggers if the inbound transmission was successful, MDN was successfully sent, MICs all match, and no other errors occurred.
- **AS2 Inbound Transaction Failed**—Triggers if the AS2 file upload failed for some reason, such as bad MIC, no permissions/ access, duplicate message ID, or other AS2 transfer-related error.
- **AS2 Outbound Transaction Succeeded**—Triggers if EFT has offloaded a file to a remote partner, and that partner replied with a receipt over HTTP/S, indicating that the transfer was successfully completed.
- **AS2 Outbound Transaction Failed**—Triggers if the expected MDN receipt was not received in the expected time or the receipt signature or MIC failed.

Type	Label (can appear in email notification)	Variable
AS2 Properties	AS2 Payload	%AS2.PAYLOAD%
	AS2 MDN	%AS2.MDN%
	AS2 Local MIC	%AS2.LOCAL_MIC%
	AS2 Remote MIC	%AS2.REMOTE_MIC%
	AS2 Message ID	%AS2.MESSAGE_ID%
	AS2 Host	%AS2.HOST%
	AS2 Transaction Error	%AS2.TRANSACTION_ERROR%
	AS2 Transaction Result	%AS2.TRANSACTION_RESULT%
	AS2 Transaction Verbose	%AS2.TRANSACTION_VERBOSE%
	AS2 Direction	%AS2.DIRECTION%
	AS2 Partner ID	%AS2.PARTNER_ID%
	AS2 EFT Server ID	%AS2.EFT_ID%
	AS2 Content Type	%AS2.CONTENT_TYPE%

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%

Type	Label (can appear in email notification)	Variable
User Properties	User (Group)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%
Connection Properties	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%

Type	Label (can appear in email notification)	Variable
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%

Cloud Object Monitor Event

The Cloud Object Monitor Event is used when you want to download files from Amazon S3, Azure blob storage, or Google Drive.

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

- Files arriving at EFT can be automatically copied/moved to cloud storage.
- Timer rules can download files from cloud storage at set intervals
- Download always uses TLSv1.2 protocol

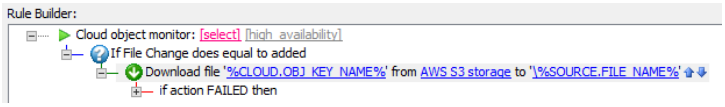
With the Cloud object monitor Event, EFT administrators can:

- Connect natively to cloud storage without scripting, manual browsing, or complexity in setting up connections
- Integrate natively with cloud storage through EFT without the need for outside integration

The Cloud Object Monitor Event does not support cloud-to-cloud (S3 to S3, Azure to S3, or S3 to Azure) direct file transfers. Currently, it can only download from the cloud to EFT, and then upload from EFT to the cloud. Timer Event Rules are also capable of downloading files from the cloud.

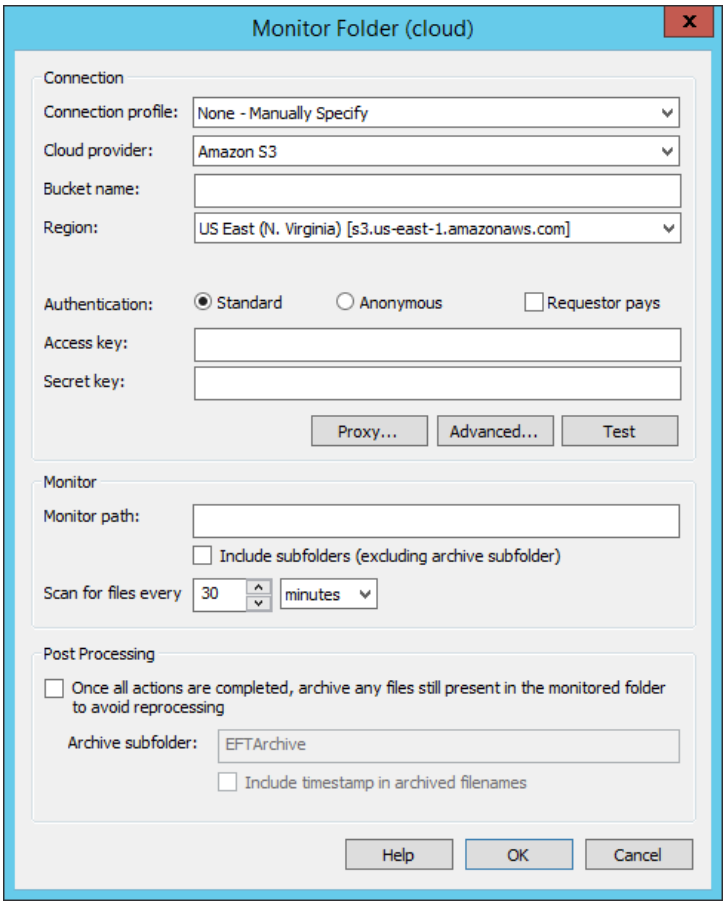
To configure a Cloud object monitor Event

1. Follow the procedure in Defining Event Rules, and to add the **Cloud object monitor** event to the Rule Builder.

   When you add the **Cloud object monitor**event to the Rule builder, an **If Change** Condition and **Download**Action are added automatically.

2. Next to **Cloud object monitor**, click **select**. The **Monitor Folder (cloud)**dialog box appears.



3. Specify the connection and authentication options described in Cloud Storage Actions.
4. If you are creating this rule on a high availability node, click **high availability**to specify the load balancing options.
5. Specify the options for the If File Change condition and the Download Action, then click **Apply**to save the event rule.

Related Topics

- Copy/Move or Download File to Cloud Storage Action
- Cloud Storage Actions
- Introduction to Event Rules
- Defining a Connection Profile
- Defining Event Rules
- Event Rule Load Balancing
- EFT Cloud Variables

Connection Events

- **User Connected**—When a user connects to the Site (this occurs before log in).
- **User Connect Failed**—When a user attempts to connect and fails (this can occur before log in).
- **User Disconnected**—When a user disconnects from the Site (this can occur before log in).

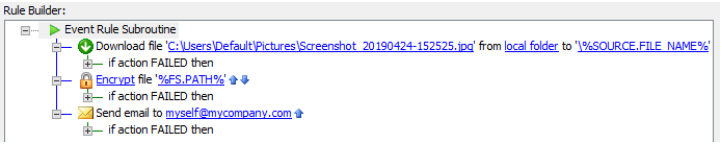
Event Rule Subroutine Event

(Requires EAM) The **Event Rule Subroutine** event is used to call another rule from the current rule to create more modular "functional" style of rules. With the **Event Rule Subroutine** event, you can build an event rule that calls a Call Event Rule Subroutine Action asynchronously, thus letting the target rule handle the burden of processing, while returning a reply immediately to the client.

Subroutines do not have conditions; when you call them, if you have multiple steps, they will all run.

To create an Event Rule Subroutine Event

1. Create an Event Ruleusing the **Event Rule Subroutine**event.
2. Add desired actions to the subroutine. For example, you could add a **Download file from host**action, **OpenPGP** action to encrypt the downloaded file, and a **Send Email notification** action to notify you when the action is complete.



3. Click **Apply**. You have created the subroutine.
4. Now you can call this subroutine in a Call Event Rule Subroutine action.

Related Topic

- Call Event Rule (GoTo) Subroutine Action

File System Events

- File Uploaded—File is uploaded to the Site.
- File Downloaded—File is downloaded from the Site.
- Verified Upload Succeeded—Integrity check of uploaded file succeeds when transferred using the Web Transfer Client.
- Verified Download Succeeded—Integrity check of downloaded file succeeds when transferred using the Web Transfer Client.
- File Renamed—File on the Site is renamed by a connected client.
- File Moved—File is moved from one folder in the VFS to another by a connected client.
- File Deleted—File is deleted from the Site by connected client
- Folder Created—Folder is created on the Site by a connected client.
- Folder Deleted—Folder is deleted from the Site by a connected client.
- Folder Changed—User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")
- Upload Failed—Upload fails to transfer successfully.
- Download Failed—Download fails to transfer successfully.
- Verified Upload Failed—Integrity check of uploaded file fails when transferred using the Web Transfer Client.
- Verified Download Failed—Integrity check of downloaded file fails when transferred using the Web Transfer Client.
- Before Download—If a download is requested, perform the Action(s) defined in this Event, then continue with the download.

Available Variables

The events above can take the following variables:

Type	Label (can appear in email notification)	Variable
AS2 Properties	AS2 Payload	%AS2.PAYLOAD%
	AS2 MDN	%AS2.MDN%
	AS2 Local MIC	% AS2.LOCAL_MIC%
	AS2 Remote MIC	%AS2.REMOTE_MIC%
	AS2 Message ID	%AS2.MESSAGE_ID%
	AS2 Host	%AS2.HOST%
	AS2 Transaction Error	%AS2.TRANSACTION_ERROR%
	AS2 Transaction Result	%AS2.TRANSACTION_RESULT%
	AS2 Transaction Verbose	%AS2.TRANSACTION_VERBOSE%
	AS2 Direction	%AS2.DIRECTION%
	AS2 Partner ID	%AS2.PARTNER_ID%
	AS2 EFT Server ID	%AS2.EFT_ID%
	AS2 Content Type	%AS2.CONTENT_TYPE%
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Virtual Path	%FS.VIRTUAL_PATH%
	Physical Path	%FS.PATH%
	Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%
	Physical Folder Name	%FS.FOLDER_NAME%
	File Name	%FS.FILE_NAME%
	Base File Name	%FS.BASE_FILE_NAME%
	File Size	%FS.FILE_SIZE%
	File Creation Date	%FS.FILE_CREATE_DATE%
	File Creation Time	%FS.FILE_CREATE_TIME%
	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%

Type	Label (can appear in email notification)	Variable
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

Type	Label (can appear in email notification)	Variable
Connection Properties	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Local Port	%CONNECTION.LOCAL_PORT%
	Protocol	%CONNECTION.PROTOCOL%
	Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%

File Downloaded	**Triggers when file is downloaded from the Site.**	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Virtual Path	%FS.VIRTUAL_PATH%
	Physical Path	%FS.PATH%
	Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%
	Physical Folder Name	%FS.FOLDER_NAME%
	File Name	%FS.FILE_NAME%
	Base File Name	%FS.BASE_FILE_NAME%
	File Size	%FS.FILE_SIZE%
	File Creation Date	%FS.FILE_CREATE_DATE%
	File Creation Time	%FS.FILE_CREATE_TIME%
	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%

File Downloaded	Triggers when file is downloaded from the Site.	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

File Downloaded	**Triggers when file is downloaded from the Site.**	
Type	**Label (can appear in email notification)**	**Variable**
Connection Properties	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Local Port	%CONNECTION.LOCAL_PORT%
	Protocol	%CONNECTION.PROTOCOL%
	Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%

Verified Upload Succeeded	**Integrity check of uploaded file succeeds when transferred using the Web Transfer Client.**	
Verified Download Succeeded	**Integrity check of downloaded file succeeds when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Virtual Path	%FS.VIRTUAL_PATH%
	Physical Path	%FS.PATH%
	Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%
	Physical Folder Name	%FS.FOLDER_NAME%
	File Name	%FS.FILE_NAME%
	Base File Name	%FS.BASE_FILE_NAME%
	File Size	%FS.FILE_SIZE%
	File Creation Date	%FS.FILE_CREATE_DATE%
	File Creation Time	%FS.FILE_CREATE_TIME%
	File CRC	%FS.FILE_CRC%
	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%

Verified Upload Succeeded	**Integrity check of uploaded file succeeds when transferred using the Web Transfer Client.**	
Verified Download Succeeded	**Integrity check of downloaded file succeeds when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

Verified Upload Succeeded	**Integrity check of uploaded file succeeds when transferred using the Web Transfer Client.**	
Verified Download Succeeded	**Integrity check of downloaded file succeeds when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
Connection Properties	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Local Port	%CONNECTION.LOCAL_PORT%
	Protocol	%CONNECTION.PROTOCOL%
	Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%

File Renamed	**File on the Site is renamed by a connected client.**	
File Moved	**File is moved from one folder in the VFS to another by a connected client.**	
File Deleted	**File is deleted from the Site by connected client**	
Folder Created	**Folder is created on the Site by a connected client.**	
Folder Deleted	**Folder is deleted from the Site by a connected client.**	
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Virtual Path	%FS.VIRTUAL_PATH%
	Physical Path	%FS.PATH%
	Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%
	Physical Folder Name	%FS.FOLDER_NAME%
	File Name	%FS.FILE_NAME%
	Base File Name	%FS.BASE_FILE_NAME%
	File Size	%FS.FILE_SIZE%
	File Creation Date	%FS.FILE_CREATE_DATE%
	File Creation Time	%FS.FILE_CREATE_TIME%
	Virtual Destination Path	%FS.DST_VIRTUAL_PATH%
	Physical Destination Path	%FS.DST_PATH%
	Physical Destination Folder Name	%FS.DST_FOLDER_NAME%
	Destination File Name	%FS.DST_FILE_NAME%
	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%

File Renamed	**File on the Site is renamed by a connected client.**	
File Moved	**File is moved from one folder in the VFS to another by a connected client.**	
File Deleted	**File is deleted from the Site by connected client**	
Folder Created	**Folder is created on the Site by a connected client.**	
Folder Deleted	**Folder is deleted from the Site by a connected client.**	
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	Groups	%USER.GROUPS%

File Renamed	**File on the Site is renamed by a connected client.**	
File Moved	**File is moved from one folder in the VFS to another by a connected client.**	
File Deleted	**File is deleted from the Site by connected client**	
Folder Created	**Folder is created on the Site by a connected client.**	
Folder Deleted	**Folder is deleted from the Site by a connected client.**	
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**	
Type	**Label (can appear in email notification)**	**Variable**
	Logon Name	%USER.LOGIN%

File Renamed	**File on the Site is renamed by a connected client.**	
File Moved	**File is moved from one folder in the VFS to another by a connected client.**	
File Deleted	**File is deleted from the Site by connected client**	
Folder Created	**Folder is created on the Site by a connected client.**	
Folder Deleted	**Folder is deleted from the Site by a connected client.**	
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**	
Type	**Label (can appear in email notification)**	**Variable**
	Logon Password	%USER.PASSWORD%

File Renamed	**File on the Site is renamed by a connected client.**	
File Moved	**File is moved from one folder in the VFS to another by a connected client.**	
File Deleted	**File is deleted from the Site by connected client**	
Folder Created	**Folder is created on the Site by a connected client.**	
Folder Deleted	**Folder is deleted from the Site by a connected client.**	
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**	
Type	**Label (can appear in email notification)**	**Variable**
	Account Enabled	%USER.ENABLED%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_ FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

File Renamed	**File on the Site is renamed by a connected client.**
File Moved	**File is moved from one folder in the VFS to another by a connected client.**
File Deleted	**File is deleted from the Site by connected client**
Folder Created	**Folder is created on the Site by a connected client.**
Folder Deleted	**Folder is deleted from the Site by a connected client.**
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**

Type	Label (can appear in email notification)	Variable
Connection Properties	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Local Port	%CONNECTION.LOCAL_PORT%
	Protocol	%CONNECTION.PROTOCOL%
	Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%

Upload Failed	**Upload fails to transfer successfully.**	
Type	**Label (can appear in email notification)**	**Variable**
AS2 Properties	AS2 Payload	%AS2.PAYLOAD%
	AS2 MDN	%AS2.MDN%
	AS2 Local MIC	%AS2.LOCAL_MIC%
	AS2 Remote MIC	%AS2.REMOTE_MIC%
	AS2 Message ID	%AS2.MESSAGE_ID%
	AS2 Host	%AS2.HOST%
	AS2 Transaction Error	%AS2.TRANSACTION_ERROR%
	AS2 Transaction Result	%AS2.TRANSACTION_RESULT%
	AS2 Transaction Verbose	%AS2.TRANSACTION_VERBOSE%
	AS2 Direction	%AS2.DIRECTION%
	AS2 Partner ID	%AS2.PARTNER_ID%
	AS2 EFT Server ID	%AS2.EFT_ID%
	AS2 Content Type	%AS2.CONTENT_TYPE%
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
	Event Reason	%EVENT.REASON%

Upload Failed	**Upload fails to transfer successfully.**	
Type	**Label (can appear in email notification)**	**Variable**
File System Properties	Virtual Path	%FS.VIRTUAL_PATH%
	Physical Path	%FS.PATH%
	Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%
	Physical Folder Name	%FS.FOLDER_NAME%
	File Name	%FS.FILE_NAME%
	Base File Name	%FS.BASE_FILE_NAME%
	File Size	%FS.FILE_SIZE%
	File Creation Date	%FS.FILE_CREATE_DATE%
	File Creation Time	%FS.FILE_CREATE_TIME%
	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%

Upload Failed	**Upload fails to transfer successfully.**	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

Upload Failed	**Upload fails to transfer successfully.**	
Type	**Label (can appear in email notification)**	**Variable**
Connection Properties	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Local Port	%CONNECTION.LOCAL_PORT%
	Protocol	%CONNECTION.PROTOCOL%
	Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%

Download Failed	**Triggers if download fails to transfer successfully.**	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
	Event Reason	%EVENT.REASON%
File System Properties	Virtual Path	%FS.VIRTUAL_PATH%
	Physical Path	%FS.PATH%
	Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%
	Physical Folder Name	%FS.FOLDER_NAME%
	File Name	%FS.FILE_NAME%
	Base File Name	%FS.BASE_FILE_NAME%
	File Size	%FS.FILE_SIZE%
	File Creation Date	%FS.FILE_CREATE_DATE%
	File Creation Time	%FS.FILE_CREATE_TIME%
	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%

Download Failed	**Triggers if download fails to transfer successfully.**	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

Download Failed	**Triggers if download fails to transfer successfully.**	
Type	**Label (can appear in email notification)**	**Variable**
Connection Properties	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Local Port	%CONNECTION.LOCAL_PORT%
	Protocol	%CONNECTION.PROTOCOL%
	Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%

Verified Upload Failed	**Integrity check of uploaded file fails when transferred using the Web Transfer Client.**	
Verified Download Failed	**Integrity check of downloaded file fails when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
	Event Reason	%EVENT.REASON%
File System Properties	Virtual Path	%FS.VIRTUAL_PATH%
	Physical Path	%FS.PATH%
	Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%
	Physical Folder Name	%FS.FOLDER_NAME%
	File Name	%FS.FILE_NAME%
	Base File Name	%FS.BASE_FILE_NAME%
	File Size	%FS.FILE_SIZE%
	File Creation Date	%FS.FILE_CREATE_DATE%
	File Creation Time	%FS.FILE_CREATE_TIME%
	File CRC	%FS.FILE_CRC%
	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%

Verified Upload Failed	**Integrity check of uploaded file fails when transferred using the Web Transfer Client.**	
Verified Download Failed	**Integrity check of downloaded file fails when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

Verified Upload Failed	**Integrity check of uploaded file fails when transferred using the Web Transfer Client.**	
Verified Download Failed	**Integrity check of downloaded file fails when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
Connection Properties	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Local Port	%CONNECTION.LOCAL_PORT%
	Protocol	%CONNECTION.PROTOCOL%
	Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%

Before Download	**If a download is requested, perform the Action(s) defined in this Event, then continue with the download.**	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Virtual Path	%FS.VIRTUAL_PATH%
	Physical Path	%FS.PATH%
	Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%
	Physical Folder Name	%FS.FOLDER_NAME%
	File Name	%FS.FILE_NAME%
	Base File Name	%FS.BASE_FILE_NAME%
	File Size	%FS.FILE_SIZE%
	File Creation Date	%FS.FILE_CREATE_DATE%
	File Creation Time	%FS.FILE_CREATE_TIME%
	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%

Before Download	**If a download is requested, perform the Action(s) defined in this Event, then continue with the download.**	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_ FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

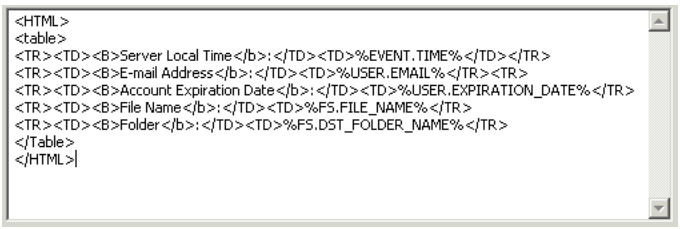
Before Download	**If a download is requested, perform the Action(s) defined in this Event, then continue with the download.**	
Type	**Label (can appear in email notification)**	**Variable**
Connection Properties	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Local Port	%CONNECTION.LOCAL_PORT%
	Protocol	%CONNECTION.PROTOCOL%
	Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%

File Uploaded Event

Suppose you want to be sent an email each time any user uploads a file to EFT, and you want to include information about the user account that uploaded the file.

To define the Event Rule

1. Create a **File Uploaded** Event Rule.
2. Add an email Notification Action.
3. In the Message of the email, add the desired user variables, such as %USER.LOGIN%, %USER.EMAIL%, and %USER.PHONE%. For example:



4. Click **Apply**.

With this very simple Rule, an email is sent whenever ***any*** user uploads a file to EFT. You can further customize the Rule to suit your needs:

- If you only want to know when a specific user uploads a file, add the Condition "If Logon name is" and select the username.
- If you only want to know when someone in a specific Group uploads a file, add the Condition "If User Groups" and select the Group.

Defining the Email with User Details

The default email body contains a table. If you can edit HTML and if the account that the email is sent to accepts HTML emails, you can format the email to suit your needs. Review your tags carefully, however, since no HTML code verification is performed by EFT.

Using the example code above, when a user with the username `jbite`uploads a file, the following email might be sent:

This message was sent to you automatically by EFT on the following Event: File Uploaded.

Server Local Time: 12/5/2007 14:00:00
email Address: jbite@mycompany.com
Account Expiration Date: 12/1/2008 11:59:59
File Name: file.txt
Folder: C:\InetPub\EFTRoot\Standard\Usr\jbite

Folder Monitor Event

(Requires FMM; in EFT Arcus, you cannot use Folder Monitor above the Site root) If you are attempting to monitor a user's home folder or one if its sub-folders, the following warning message appears:

"It appears you are attempting to monitor a user's home folder or one if its sub-folders. For detecting protocol-based file uploads, we strongly encourage the use of the File Upload trigger, rather than a Folder Monitor trigger. The Folder Monitor trigger relies on Window's notification events, which will occur as chunks of the file are uploaded. The resulting downstream effect is a race condition where actions associated with this event rule may fire BEFORE the file has been completely uploaded. We recommend only using Folder Monitors for monitoring LAN file copy events."

The EFT **Folder Monitor** Event Rule trigger is used to detect the creation, deletion, and renaming of files in a monitored folder and to perform Actions based on these triggers. You can use a **Folder Monitor** Rule to trigger when files are added to a folder using the network file system. When monitoring folders for files added to EFT via the FTP/S, SFTP, and HTTP/S protocols, use File Uploaded, File Downloaded, and other File Server Events. Folder Monitor Rules are not fired for Events happening to folders such as the addition, renaming, or removal of a folder; it only applies to ***file***changes within the folder or subfolders.

The Folder Monitor Rule can pass Unicode filenames to the Event Rule system, including the Advanced Workflow Module, Custom Commands, text-based log files, and ARM. The Unicode filename will be saved in the auditing database, but the reporting tool cannot display Unicode filenames.

Folder Sweep

Occasionally, file system notification will fail (for example, due to network errors), so files added to the monitored folder are missed and not processed (for example, not moved to another location) if the Rule is using only notifications to detect files. After the Folder Monitor Rule is created, the Event Rule system can periodically poll the monitored folder (and subfolders, if specified) to ensure that all files have been processed. This "Folder Sweep" feature is allowed only for "file added" Actions. The Folder Sweep polling occurs at a user-specified frequency. Immediately upon Site or Event Rule start, the initial polling occurs and will trigger any Actions added to the Rule. Folder Sweep is enabled by selecting the **Scan for files every** check box in the **Monitor Folder** dialog box. If the check box is not selected, the associated frequency controls are disabled. Refer to the procedure below for instructions for enabling Folder Sweep.

A new Event type named "Folder Monitor – sweep" is defined and used to populate the `eventType` field in the auditing database when reporting Folder Monitor Rules that

were triggered because of Folder Sweep. Also, the Folder Sweep archiving of files will be recorded using the EVENT_ACTIONS value of EVENT_ACTION_FS_ARCHIVED.

The following table describes the Folder Sweep information entered in the log:

Log Level	Event

Debug	• When a Folder Monitor Rule starts execution, log which triggering mechanism(s) are being employed and whether subfolders are being monitored. Also log:
	  ◦ If folder sweep is on, show frequency, time units, and archive subfolder name.
	  ◦ If RDCW* is on, show whether health check is on and its frequency.
	• When a monitored folder is polled for its contents with special indication for the first poll.
	• Log which mechanism, RDCW notification or folder polling, triggers the processing of a file.
	• Log when file has been archived.
	• Log when file is still in folder after Event Rule Actions have completed and user chose not to archive.
	• Record trigger collisions by logging if Event is being ignored because file is already in process.
	• For folder sweep, log when folder contents have been received and are about to be processed.
	
	*RDCW = ReadDirectoryChangeWrite function; Retrieves information that describes changes within a specified directory.

Error	• Log reason for archive folder creation failure. • Log reason for file archive Action failure.

Risks associated with Folder Sweep include:

- EFT creates a handle for EVERY file polled (when **Scan for files every *n*** is selected). You can use an "If File Name" or "If Base File Name" Condition to include or exclude file name or extension or wildcard characters (for example, "*.txt" or "File??.dat"). Using the Condition prevents EFT from opening a file handle for each of the excluded files, which provides a slight performance improvement.
- If you do not use the archive feature and the file is not removed from the Monitored Folder due to an Action failure, the file will be reprocessed in the next Folder Sweep cycle.

- If the Health Check fails, it is possible to see duplicate Folder Monitor errors in the log.
- If the Event Rule has been placing files in the Archive subfolder specified in the Folder Monitor and then you change the name of the Archive subfolder, files that were previously archived by Folder Sweep will be reprocessed.
- If multiple Folder Monitor Rules point to same folder, a "race condition" can occur when the two Rules attempt to concurrently process the same file.
- Folder Monitor does not trigger when Unicode filenames are added to the monitored folder; however, Folder Sweep archives them. Refer to Unicode Support in EFT for more information.
- EFT must have permission to access the folder (see note below). If the folder specified is not accessible by EFT, an error message appears. (For information about system error codes, refer to https://docs.microsoft.com/en-us/windows/win32/debug/system-error-codes--0-499-)
- If you are sending files to an ICAP server in batches for scanning using the Content Integrity Control Action, you might not get consistent results. It is not recommended to use the Folder Monitor event for scanning files with the Content Integrity Control Action. Instead, use the File Uploaded event.

Archiving

After all Folder Monitor Rule Actions have been executed and if the archive option is enabled, the Folder Monitor Rule will determine whether a file is still in the monitored folder. For this reason, Rule Actions are forced to Stop processing so that execution returns to the Rule only after all Actions have finished. If the file is still in the folder, the Folder Monitor Rule creates the **Archive**subfolder (if not there already) in the folder containing the file to be archived. If an error occurs while creating the **Archive** subfolder, a message containing the failure reason will be logged; otherwise, the file is moved from the monitored folder into the **Archive**subfolder. If an error occurs during archival, a message containing the failure reason is logged. Whatever the reason, if a file's archival fails, the file is left alone.

If the archive feature is not enabled, files are left in the monitored folder, if Event Rule Actions have not otherwise disposed of them. Archive folders will have the same permissions as their parent folders and will not be given special attributes for connecting clients.

Creating a Folder Monitor Rule

EFT keeps track of the number of active threads over time and periodically calculates the average number of concurrent active threads during that time. The sample rate is once every 5 seconds, and the sample period is 10 samples. After sampling 10 times and finding the average concurrent active threads over that period, the system can grow the pool of the concurrent active threads, up to a set maximum number of threads. This means that if EFT is currently running close to or above the prior average of concurrent threads, it will grow the thread pool to allow for room for more Events. By default, EFT starts with 3 threads in the pool per Site, and can grow to a maximum of 32 threads.

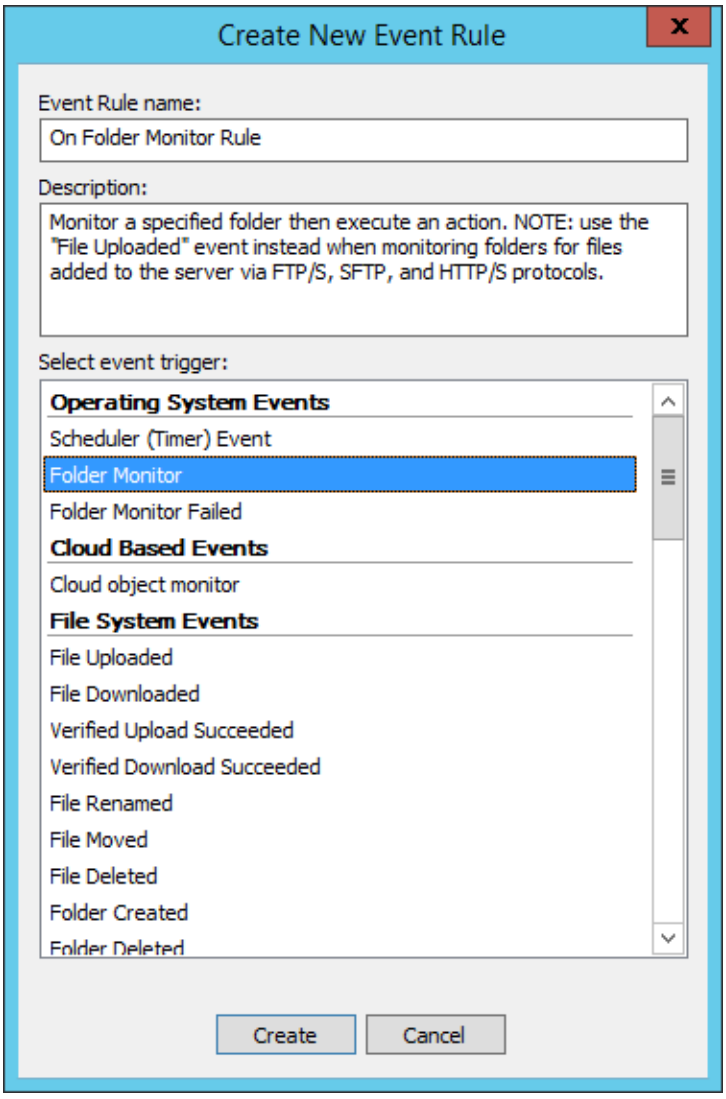
EFT will only reset affected (modified) folders when applying configuration changes to an Event Rule, rather than resetting all folders.

When monitoring a folder, EFT watches for any file being added to, removed from, or renamed in the monitored folder. Moving a file, performing OpenPGP operations, and other Actions can trigger the Rule again, resulting in failures. This can be avoided by selecting the **Stop processing this rule** check box after **if action failed then**.

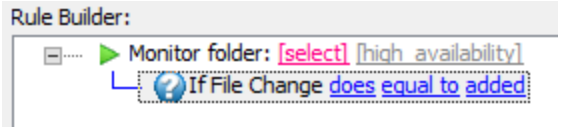
The **Require Active Directory domain trust relationship** check box is cleared by default for new installs and selected by default during upgrades if the advanced property **FolderMonitorUseNonInteractiveLogon**is present during the upgrade. The **Scan for files every** check box is not selected and associated controls are disabled. All other control settings are carried over from existing Rules during upgrade (health check yes/no and rate, subfolders yes/no, login credentials).

To configure a Folder Monitor Rule

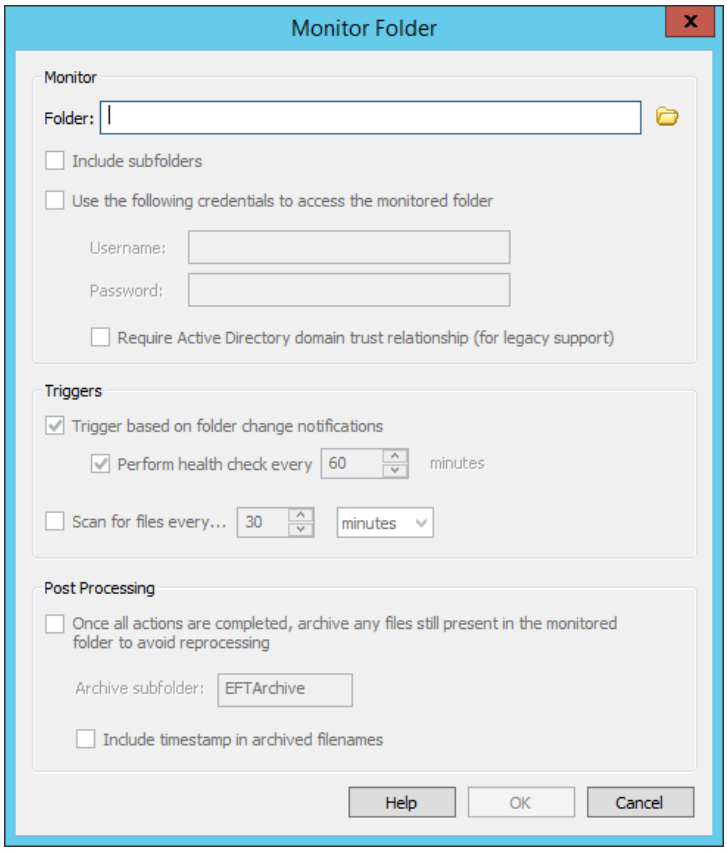
1. Open the Create New Event Rule dialog box.
2. In the **Create New Event Rule** dialog box, click **Folder Monitor**, and then click **Create**.



The new, blank Rule appears in the **Rule Builder**.



3. In the Monitor folder Event, click **[select].**The **Monitor Folder** dialog box appears.



Next to the **Folder**box, click the folder icon to specify a folder to monitor.

To monitor a folder on a remote, non-EFT file server, supply the full **UNC** path to the network share. (The format for a UNC path is **\\server\volume\directory** and is not case-sensitive. For example: **\\Shared1_ svr\Shared1\WGroups\Network**).

Make sure that the EFT service has sufficient privileges to perform READ operations on the remote share.

If you are using the "health check" feature, it must also have WRITE permissions.

This is generally easiest if you set the EFT service to run as a domain account, or specify a dedicated “run as” account in the **Monitor Folder**dialog box.

Wildcards are not supported; however, you can use an "If File Name" or "If Base File Name" Condition to include or exclude file name or extension or wildcard characters (for example, "*.txt" or "File??.dat"). Doing so prevents EFT from opening a file handle for each of the excluded files, which provides a slight performance improvement.

4. If you also want to monitor subfolders, select the **Include subfolders** check box. For example, if you are monitoring a user folder and the user has created subfolders, unless you select the **Include subfolders** check box, files added to or changed in subfolders do not trigger the Rule.
5. If login credentials (other than the EFT server service account) are required to access the folder and subfolders, select the **Use the following credentials to access the monitored folder** check box, then specify the username and password.

   The Microsoft definitionof noninteractive login states: “Noninteractive authentication can only be used after an interactive authentication has taken place. During noninteractive authentication, the user does not input logon data; instead, previously established credentials are used. Noninteractive authentication is the mechanism at work when a user connects to multiple computers on a network without having to re-enter logon information for each computer.” In this case, EFT has joined the domain and/or the server service runs as a domain user. You could supply different credentials to run as a different user for this Action.

   The **Require Active Directory domain trust relationship** check box specifies how the Folder Monitor Event Rule will log in to monitor remote folders. Selecting this check box indicates that Folder Monitor must establish a "trustful" connection to the system containing the folder(s) being monitored. This control is not enabled unless the **Use the following credentials to access the monitored folder** check box is selected. (Please also refer to the note above regarding this check box.)

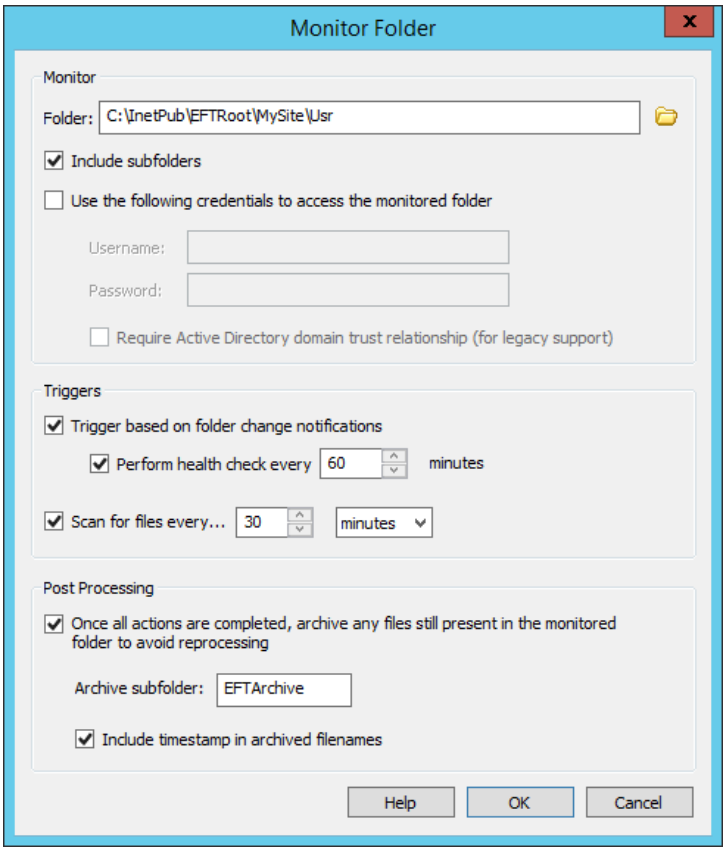
6. In the **Triggers**area, select the **Trigger based on folder change notifications** check box to cause Events to be set off by the receipt of directory change notifications (add, delete, and rename) generated by the system.
7. To monitor the status of the network connection and report failures, select the **Perform health check every** check box, and specify an interval. An hour (60 minutes) is specified by default.

   When the check box is selected, EFT periodically writes a special file to the folder specified and then waits for the "file added" notification to verify that it can receive notifications of changes within the folder. When there is a loss of connectivity, EFT attempts to re-establish a link to the folder and triggers the Folder Monitor Failed Event internally.

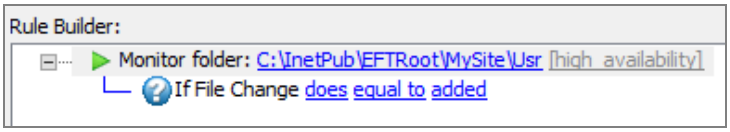
   - If you want to receive email failure notifications (or other Actions) when the Folder Monitor health check returns a connection failure, create an additional Event Rule using the **Folder Monitor Failed**Event, and add the **Send notification email** Action to it.

The time EFT waits for the notification from Windows when a Folder Monitor health check file is created can be controlled by an advanced property described in https://kb.globalscape.com/KnowledgebaseArticle10682.aspx.

8. To enable Folder Sweep, select the **Scan for files every** check box and specify the frequency. The default is 30 minutes. A value between 1 and 9999 can be specified with units of seconds, minutes, or hours. The timer for the next sweep cycle is not started until all the files for the current sweep cycle have processed through all Event Rule Actions. Folder Sweep limits its processing to 1000 files at a time. If the monitored folder contains more than 1000 files, up to 1000 of the remaining files will be processed during the next sweep cycle. Selecting the **Scan for files every** check box will cause a Folder Monitor scan upon Event Rule start up (such as when you create the Rule and then click **Apply**). If you have Actions in the Rule, such as an email notification, those Actions will be triggered. (This check box is not selected by default.) Selecting the **Scan for files every** check box causes the Event Rule's **If File Change** Condition to be set to **does equal to added**.
9. All files in a monitored folder will be processed every sweep cycle so if a user neglects to remove processed files or if a Rule Action that was supposed to remove the file fails, the file will be reprocessed. In the **Post Processing** area, select the **Once all actions are completed, archive any files still present in the monitored folder to avoid reprocessing** check box, and then specify the name of the folder in which to archive any remaining files. The default is `EFTArchive`. The **Archive** subfolder will reside directly under the folder in which the file was added. The **Archive** subfolder name cannot contain any of the following characters: `| / \ ? * < " : > + [ ]` and is limited to 248 characters. (The total cannot exceed Windows path limit.)
    - Select the **Include timestamp in archived filenames** check box to avoid overwriting any files of the same name in the **Archive**subfolder. The file name will be appended using the Event Rule variables %EVENT.DATESTAMP% and %EVENT.TIMESTAMP_PRECISE% (time to the millisecond).
    - If Folder Sweep is enabled and you have specified an **Archive**subfolder, the **Archive**subfolder is ignored when **Include subfolders** is enabled.
    - If you change the name of the **Archive** subfolder, the existing **Archive** subfolders will be unaltered. If processing of subfolders is enabled, notifications and polling for contents of the former **Archive**subfolders will begin immediately upon applying the Rule changes.



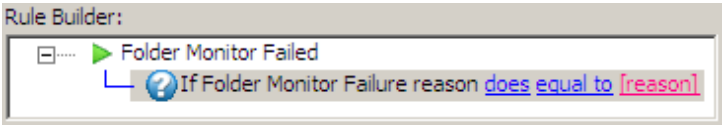
10. Click **OK**. If the **Once all actions** check box is selected and an invalid name or no name is given for the **Archive** subfolder, it will revert to the default name (`EFTArchive`) and a warning message appears.
11. The **If File Change**Condition is added automatically to restrict the triggering of the Rule. Click the links in the **If File Change** Condition to specify whether the Rule should trigger when a file in the folder is or is not renamed, added, or removed. If Folder Sweep (the **Scan for files every** check box) is enabled (as described above), the **If File Change** Condition is forced to **does equal to added** because Folder Sweep only applies to files added to a folder or subfolders.
12. Specify any Action/Conditions to occur when this Event is triggered, such as:
    - Add an email notification. (Refer to email Notification Action.)
    - Copy or move a file added to the monitored folder to another location. (Refer to Copy/Move File to Host Action.)
    - Add Conditions, such as the **If File Change**Condition so that the Rule doesn't trigger again after the file is moved or renamed. (Refer to Using Conditions.)



11. Click **Apply**to save the changes on EFT.

Folder Monitor Failure

To audit failures of Folder Monitor Rules, use the **Folder Monitor Failed** Event, then add the **If Folder Monitored Failure reason**Condition.



- Click the **reason** link to specify a failure reason that will trigger the Rule: **any failure**, **archive failure**, **health check failed**.

Folder Monitor archive folder errors will also trigger this Event and write to the Windows Event log.

GDPR Right Exercised

The **GDPR Right Exercised** event is triggered based on the **If Event Reason**Condition specified. You can specify that the Event Reason "does" or "does not" equal one of the following behaviors:

- The user has rescinded consent
- The user has accessed (viewed) their personal data
- The user has had rectified (modified) their personal data
- The user has asked to be forgotten
- The user has asked to restrict the use of their personal data
- The user has asked to restrict the use of their personal data
- The user's personal data has been modified by someone other than the user
- The user has ported (exported) their personal data
- The user has objected to the use of their personal data

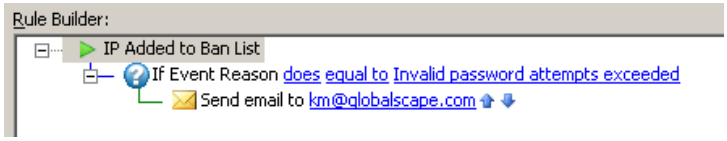
For example, you could define an Event Rule to send an email notification when a user's personal data is modified by someone other than the user, such as an administrator.

IP Added to Ban List Event

This Event is triggered when an IP address is added to the ban list by the system (not manually by an administrator). Administrators can configure Event Rules to capture this Event and send notifications or write to logs.

To define an IP Added to Ban List Event

1. Follow the procedures in Defining Event Rules.
2. In the **Create New Rule** dialog box, under **Site Events**, click **IP Added to Ban List**, and then click **OK**. The new Rule appears in the **Rule Builder**.
3. Add any (optional) Conditions(for example, If Event Reason, If Remote IP, If Server Running, etc.) and one or more Actions (for example, Send notification email).
    - The possible Event Reasons include DoS/Flood prevention trigger (permanent or temporary), Invalid password attempts exceeded, and Invalid username attempts exceeded.
4. Click **Apply**to save the Rule. The Rule appears similar to the Rule below.



IP Access-related Event Rules are limited to 50,000 rules. This can be increased with the advanced properties IPRulesLimit and AutobanLimit, however, you could experience performance issues at higher limits.

If the limit is reached, rather than not adding the IP, EFT performs a FIFO operation, adding the newly banned IPs, and removing the oldest banned IP (ONLY for auto-banned IPs; manually added IPs cannot be automatically removed.)

If an IP had to be removed, a WARNING is sent to the eft.log, indicating that a new IP has been added, and oldest IP has been dropped as the list is full. The DMZ Gateway has a correspondingly large list to handle any IPs passed to it by EFT.

Refer to the Knowledgebase article https://kb.globalscape.com/Knowledgebase/10877/Adjust-IP-Access-Rule-Count-Limit-and-IP-Auto-Ban-List-limit for more information.

Operating System Events

The operating system events below are available in EFT:

- Scheduler (Timer)—Execute a specified Action one time or repeat at a specified interval. (Requires TEM)
- Folder Monitor—Monitor a specified folder, then execute an Action whenever a change is detected. (Requires FMM)
- Folder Monitor Failed—Monitor a specified folder, then execute a specified Action whenever a failure is detected. (Requires FMM)

Use the **File Uploaded** file system Event to notify you when a file is uploaded to the Site.

Available Variables

Scheduler (Timer)

Execute a specified Action one time or repeat at a specified interval. (Requires TEM)

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%

Type	Label (can appear in email notification)	Variable
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_ MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_ DIRECTORY%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%

Folder Monitor

Monitor a specified folder, then execute an Action whenever a change is detected. (Requires FMM) Use the **File Uploaded** file system Event to notify you when a file is uploaded to the Site.

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%

Type	Label (can appear in email notification)	Variable
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	File Change	%FS.MONITOR_OPERATION%
	Physical Path	%FS.PATH%
	Physical Folder Name	%FS.FOLDER_NAME%
	Base File Name	%FS.BASE_FILE_NAME%
	File Name	%FS.FILE_NAME%
	Physical Destination Path	%FS.DST_PATH%
	Physical Destination Folder Name	%FS.DST_FOLDER_NAME%
	Destination File Name	%FS.DST_FILE_NAME%
	Virtual Path	%FS.VIRTUAL_PATH%
	Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%
	Virtual Destination Path	%FS.DST_VIRTUAL_PATH%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%

Folder Monitor Failed - Monitor a specified folder, then execute a specified Action whenever a failure is detected. (Requires FMM)

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Folder Monitor Health	%EVENT.MONITORHEALTH%
	Folder Monitor Failure Reason	%EVENT.MONITORFAILUREREASON%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	Physical Path	%FS.PATH%
	Physical Folder Name	%FS.FOLDER_NAME%
	File Name	%FS.FILE_NAME%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%

REST Invocation Event

(Require EAM and HTTPS) The REST Invocation event is used to call up a specific endpoint, such as a remote webhook, or for non-administrative users to execute an event rule for inbound traffic.

> **NOTE:** You do NOT need the REST API enabled to use this event trigger

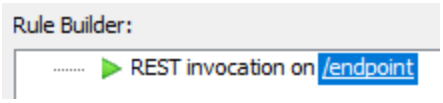
If you are using a PowerShell script for the authentication or verification, The PowerShell authentication script has to set the HTTP.AuthSuccess variable to "true." The PowerShell script for signature checking has to set the HTTP.SignatureValid variable to true.

This new feature has nothing to do with the internal REST API functionality, but instead allows EFT administrators to expose or create "endpoints" that when accessed will trigger defined actions within the event rule. Additionally, the requests will go through either the HTTP or HTTPs protocol and NOT via our REST API protocol.

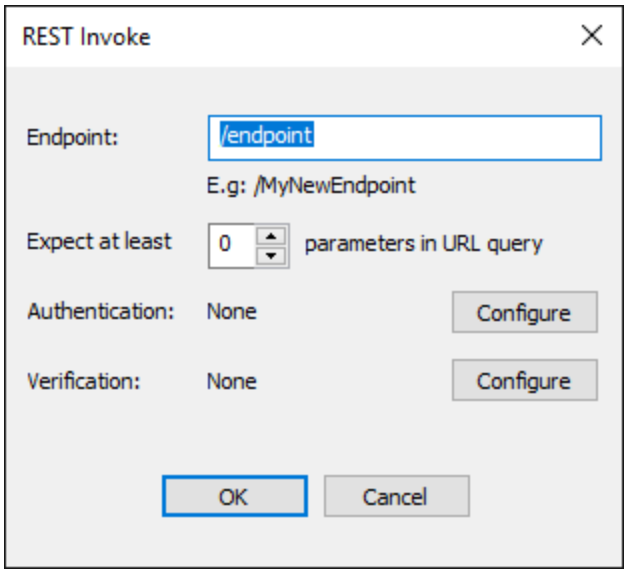
See also the sample PowerShell actionfor REST invocation, EFT response, and The list of variables EFT populates below.

To use the REST Invocation Event

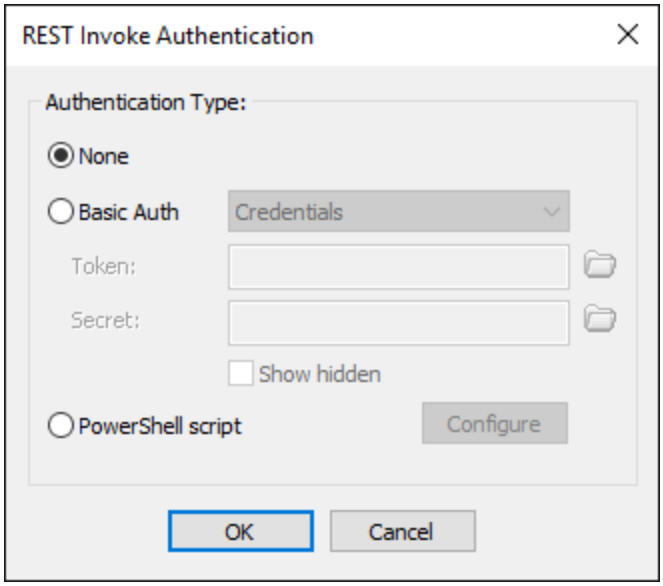
1. Ensure HTTPS or HTTP is enabled. If neither port is enabled, the event rule cannot be created and a warning or err
2. Define an Event Rule using the **REST Invocation** Event trigger. The Event trigger appears in the Rule Builder.



3. Click the linked text, /endpoint, to open the **REST Invoke** dialog box.

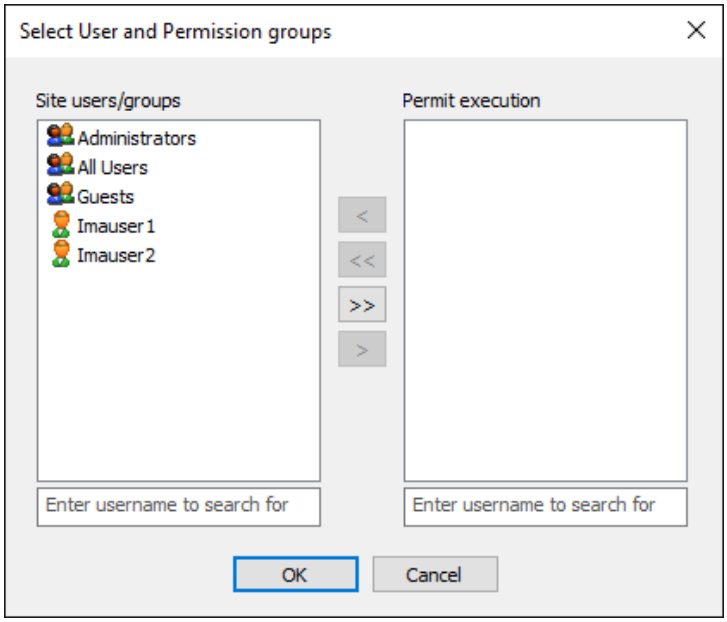


4. In the **Endpoint**box, provide the name of the endpoint.
5. In the **Expect at least** box, provide the number of parameters required in the URL query. When this is defined, the Invoke would only trigger if the set amount of URL parameters are passed, For example https://192.168.100.165/endpoint?Value&Value2&Value3 is passing three parameters in the URL. If **Expect at least** is set to 2, then this would trigger the event rule because it at least 2 parameters are passed (but you can pass as many as you need).
6. For **Authentication**options, click **Configure**. The **REST Invoke Authentication** dialog box appears.



7. Under **Authentication Type**, click an option:

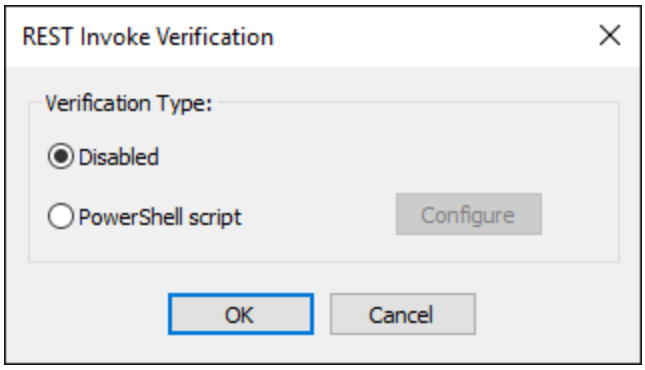
- **None** - No authentication is required. When configured for None, any call to the EFT server that contains the endpoint will trigger the event rule.
- **Basic Auth**- Use Basic authentication:
  - **Credentials**, provide the **Token**and **Secret**. (Copy and paste the token and secret generated by the provider, such as Twilio. They are case sensitive.) When using token/secret you must pass the defined token/secret within the URL request to the EFT server.
  - **Clients and Permission Groups**, click the folder icon, then move the **Site user/groups**that you want to **Permit Execution**. User/Group supports EFT users or groups defined in EFT.



- **PowerShell script**- Click **Configure** and then point to a PowerShell script. The PowerShell script has to set the HTTP.AuthSuccess variable to "true":

  $EFT_CONTEXT.SetVariable("HTTP.AuthSuccess", "true")

8. For signature **Verification**options, click **Configure**. The **REST Invoke Verification**dialog box appears.



9. The default is **Disabled**. To specify a different verification type. click **PowerShell script**, click **Configure**to select your script. then click **OK**. (The PowerShell script for signature checking has to set the HTTP.SignatureValid variable to "true." See the sample below.
10. Add Conditions(optional) and Actions(for example, Send email or write to a file), then click **Apply**.

EFT Response

The response includes an HTTP response code, and optionally, JSON payload with modified context variables.

By default, EFT responds with "200 OK." To modify the response code, set the `HTTP.Response.Code`variable. The body goes to `HTTP.Response.Body`.

EFT populates the following context variables

URL query:

- HTTP.Request.Url.Query -- Raw query
- HTTP.Request.Url.Query.Count -- number of items in the query
- HTTP.Request.Url.Query[1] -- the first item (e.g file=untitled.txt)
- HTTP.Request.Url.Query[1].Key -- the first item name (eg "file")
- HTTP.Request.Url.Query[1].Value -- the value of the first item (e.g. "untitled.txt")
- HTTP.Request.Url.Query[file] -- the value of the item named "file"

For the query items in the body (for POST requests with the content-type: application/x-www-form-urlencoded)

- HTTP.Request.Body.Query
- HTTP.Request.Body.Query.Count

- HTTP.Request.Body.Query[1]
- HTTP.Request.Body.Query[1].Key
- HTTP.Request.Body.Query[1].Value
- HTTP.Request.Body.Query[file]
- HTTP.Request.Raw -- the whole request
- HTTP.Request.Verb -- HTTP verb (GET, PUT, POST etc)
- HTTP.Request.Url -- full path including query string
- HTTP.Request.Url.Endpoint only endpoint path (e.g up to the '?' character if present)
- HTTP.Request.Headers.Count -- total number of headers
- HTTP.Request.Headers.Raw -- all headers separated by newline character
- HTTP.Request.Headers[content-type] -- a header value by name
- HTTP.Request.Headers[1] -- the first header name and value
- HTTP.Request.Headers[1].Key -- the first header name
- HTTP.Request.Headers[1].Value -- the first header value
- HTTP.Request.Body.Raw -- raw body of the request
- HTTP.Request.Body.Json.user.name -- value of the JSON payload (if present) by name. here you access the user.name field. Array fields are accessible via brackets like in javascript (e.g userrs[3])

Sample PowerShell action

Below is a sample PowerShell action that retrieves all context variables and outputs them back as a JSON, which you can use for testing.

```
$urlquery = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query")

$urlqueryCount = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query.Count")

$urlfirstQueryItemByNumber = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query[1]")

$urlfirstQueryItemByNumberKey = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query
[1].Key")

$urlfirstQueryItemByNumberValue = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query
[1].Value")

$urlfirstQueryItemByName = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query[a]")

$bodyquery = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query")
```

```
$bodyqueryCount = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query.Count")

$bodyfirstQueryItemByNumber = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query[1]")

$bodyfirstQueryItemByNumberKey = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query
[1].Key")

$bodyfirstQueryItemByNumberValue = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query
[1].Value")

$bodyfirstQueryItemByName = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query[c
 x]")

$HttpRequestRaw = $EFT_CONTEXT.GetVariable("HTTP.Request.Raw")

$Verb = $EFT_CONTEXT.GetVariable("HTTP.Request.Verb")

$Url = $EFT_CONTEXT.GetVariable("HTTP.Request.Url")

$Endpoint = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Endpoint")

$headersCount = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers.Count")

$headersRaw = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers.Raw")

$ContentType = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers[content-type]")

$FirstHeader = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers[1]")

$FirstHeaderKey = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers[1].Key")

$FirstHeaderValue = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers[1].Value")

$BodyRaw = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Raw")

$BodyJsonFirstItem = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Json.first")

$response = @{

    urlQuery=$urlQuery

    urlFirstQueryItemByNumber=$urlFirstQueryItemByNumber

    urlFirstQueryItemByNumberKey=$urlFirstQueryItemByNumberKey

    urlFirstQueryItemByNumberValue=$urlFirstQueryItemByNumberValue
```

```
    urlFirstQueryItemByName=$urlFirstQueryItemByName

    bodyQuery=$bodyQuery

    bodyFirstQueryItemByNumber=$bodyFirstQueryItemByNumber

    bodyFirstQueryItemByNumberKey=$bodyFirstQueryItemByNumberKey

    bodyFirstQueryItemByNumberValue=$bodyFirstQueryItemByNumberValue

    bodyFirstQueryItemByName=$bodyFirstQueryItemByName

    HttpRequestRaw=$HttpRequestRaw

    Verb=$Verb

    Url=$Url

    Endpoint=$Endpoint

    Headers=$Headers

    ContentType=$ContentType

    FirstHeader=$FirstHeader

    FirstHeaderKey=$FirstHeaderKey

    FirstHeaderValue=$FirstHeaderValue

    BodyRaw=$BodyRaw

    BodyJsonFirstItem=$BodyJsonFirstItem

}

$json = $response | ConvertTo-Json

$EFT_CONTEXT.SetVariable("HTTP.Response.Body",
 $json)
```

Examples

In development testing and QA, we used curl to make HTTP or HTTPs calls to the EFT Server.

Making an HTTP REST request using curl:

HTTPs: When using HTTPs and a self signed certificate, curl will be unable to accept the certificate; therefore, you will need to add --insecure to the request, as shown below.

```
curl.exe --insecure
https://<username>:<password>@<IP>:<PORT>/<endpoint>

curl.exe --insecure https://Ivan:test@192.168.100.165:443/QA
```

HTTP:

```
curl.exe http://<username>:<password>@<IP>/<endpoint>

curl.exe http://Ivan:test@192.168.100.165/QA
```

Passing parameters via the request:

In order to pass multiple parameters, the endpoint needs to include them: Multiple query string parameters via curl - Squirrel Code - Electric Imp Forums

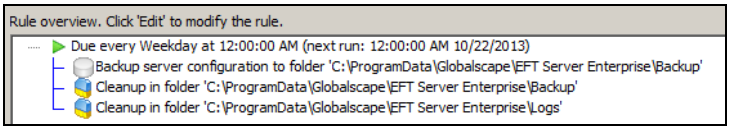
For example if you set EFT to expect at least 5 URL requests, then the curl request would be as follows:

```
curl --insecure
"https://192.168.100.166:443/QA?One&Two&Three&Four&Five"
```

Scheduler (Timer) Event

(Requires TEM) The **Scheduler (Timer) Event**allows you to execute a specified Action (e.g. send an email or a report) only one time or to repeat at specified intervals. For example, you could schedule the Cleanup in folder Action to occur on July 8 at midnight, or every Monday morning, or on the last Friday of every month at 2 a.m.

The PCI DSS requires that you develop a data retention and disposal policy. With the Cleanup in folder Action, you can configure EFT to clean up a specified folder at regularly scheduled intervals. If **Strict security settings for compliance with PCI DSS** was selected during Site setup, the **Data Retention and Disposal** dialog box appears in which you can create a **Scheduler Timer Event** with the **Clean-up**Action to delete files matching the expressions you specify. You can also choose to define it in the administration interface on existing Sites.

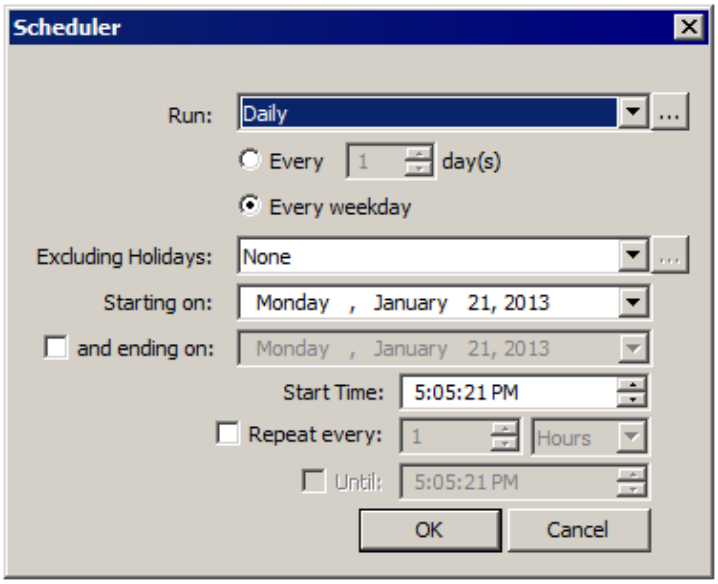


A recurring Timer does not stop recurring if the Rule Actions fail; it will recur as scheduled until you disable or delete the Rule. For example, suppose you want to download a file from a remote server, delete the file from the remote location after transfer, then send yourself an email. If the file that you want to download is not yet in the remote directory, the Rule will fail for that particular instance of the Timer running, but it will run again at the next scheduled time (for example, every four hours). In the case of Timer Rules, "Stop processing this rule" means "do not execute any further Actions with this Rule" (such as sending an email), but it does NOT mean that the Timer will stop. For example, if you have defined the Rule to run every hour, the Timer Rule will fail when the file is not in the remote location, but the Timer Rule will run again the next hour, and the next hour, and so on, until you tell it to stop (by manually disabling it).

The "Run On One of" feature in Event Rules currently only supports computer (NetBIOS) names. Refer to Event Rule Load Balancing for more information about the "Run On One of" feature.

To define a Timer Rule to download a remote file

1. Follow the procedure in Creating Event Rules.
2. In the **Create New Rule** dialog box, click **Scheduler (Timer) Event**, and then click **OK**. The new Rule appears in the **Rule Builder**.
3. To specify the start date, start time, recurrence pattern, and/or interval, in the **Rule Builder**, click the link. The **Scheduler**dialog box appears.



4. In the **Scheduler**dialog box, specify the parameters of the Timer Event: the **Run** frequency, whether to exclude holidays, when the Event should start, date the Event should end (optional), time the Event should end (optional), and recurrence frequency (optional). (When the End date is reached, the Rule will remain active in the Event Rule list, but will no longer execute any Actions.)

   The **Run** options include the following frequencies. The dialog box options change depending on your selection in the Run box.

   - **Once**—The event runs one time at a specified date and time, and never repeats. (for example, Monday, September 27, 2010 at 8 AM.)
   - **Continually**—The event starts at a specified date and time and repeats every <n> **Hours**, **Minutes**, or **Seconds**. (for example, Monday, September 27, 2010 at 8 AM and every hour thereafter.)
   - **Daily**—The event runs every <n> days or every weekday, starting at a specified date and time, and ending on a specified date and time or repeating every <n> hours, minutes, or seconds. You can also exclude certain holidays and/or end the recurrence of the event at a specified date and time. (for example, Every weekday, excluding US holidays, starting Thursday, Monday, September 27, 2010 at 8 AM and every hour thereafter.)

- **Weekly**—The event runs every <n> weeks on a specified day(s) of the week, starting at a specified date and time and ending on a specified date and time or repeating every <n> hours, minutes, or seconds. You can also exclude certain holidays and/or end the recurrence of the event at a specified date and time. (For example, Every 2 weeks on Monday at 8 AM starting on Monday, September 27, 2010, with no defined end date.)
- **Monthly**—The event runs on the <n> day of every <n> month(s) or the <nth> day of the week of <n> month(s) starting at a specified date and time and ending on a specified date and time or repeating every <n> hours, minutes, or seconds. You can also exclude certain holidays and/or end the recurrence of the event at a specified date and time. (for example, The first day of every month, starting on Friday, October 1, 2010 at 8:00:00 AM, excluding US holidays with no defined end date.)
- **Yearly**—The event runs every <month> <day> or on the <n> <day of the week> of <month> starting at a specified date and time and ending on a specified date and time or repeating every <n> hours, minutes, or seconds. You can also exclude certain holidays and/or end the recurrence of the event at a specified date and time. (for example, The first Monday of December, starting on Monday, December 6, 2012 at 8:00:00 AM, excluding US holidays with no defined end date.)
- **Custom**—The **Run Day Calendar** appears in which you can specify a date. (Past dates are not available.)
    - Click to select the date(s) to run the event. Selected dates are highlighted in green. Click the date again to clear it.
    - Click the right arrow to advance the calendar to the next year; click the left arrow to go back. Or click the name of a month to display the same month in subsequent years. With the month name selected, move the cursor up or down to scroll through the years, then release the cursor to select the year. (For example, click October 2010 to jump to October 2012. The entire calendar jumps, not just the selected month.)
    - The **Propagate selected date(s) to all subsequent years** check box is selected by default. Clear the check box if you do not want the event to run on the same date every year.
    - After you select one or more dates to run the event, you can save the schedule by clicking **Save**. In the **Save Calendar**box that appears, provide a name for the calendar, and then click **OK**. The calendar is saved and its name appears in the **Run**box. You can edit your custom calendar by click the ellipsis button next to the **Run**dialog box. (Up to 100 custom calendars can be saved and/or displayed in the **Run** box.)

- You can **Export**your custom calendar (as <name>.csv) and **Import** custom calendars. After importing a custom calendar, you can use **Save As** to save it with a new name, **Rename**it, or **Delete** it from your custom calendars. (A confirmation prompt appears when you click **Delete**.)
- You can create up to 100 custom calendars.

5. Click **OK** to save your changes. The event is updated in the **Rule Builder**.
6. Specify the Action to occur when this event is triggered.
7. Click **Run Now** to test your Rule.

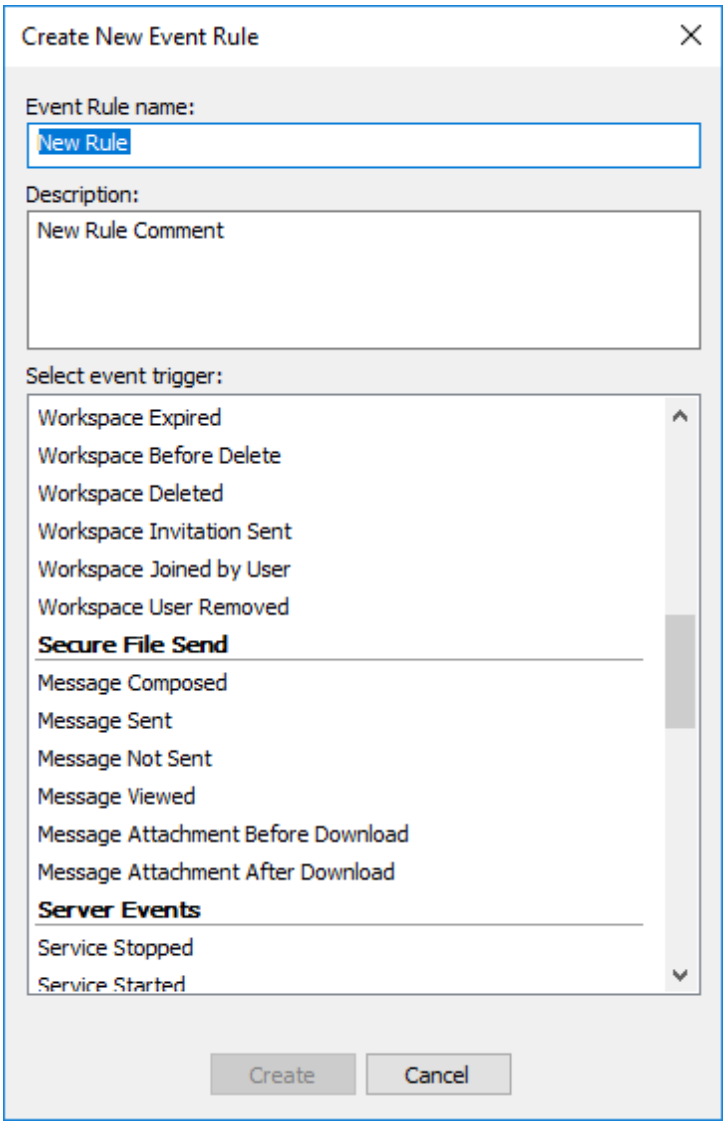
   When you create a Timer Rule, the **Run Now** button appears at the bottom of the **Rule Builder**. When you click **Run Now**, EFT executes any actions associated with the event, and any Rule construction errors are identified. You cannot perform any other operations in the EFT administration interface while EFT tests the Rule. Multiple Actions defined in the Rule, such as move, copy, or download, take longer to test than other operations such as email notifications.

   If there are no errors, a confirmation message appears asking you to verify the expected outcome. Click **Continue** to execute the Rule or **Cancel** to refine the Rule.

8. Click **Apply** to save the changes on EFT.

Secure File Send Events

Secure File Send events are "ad hoc" triggers used in event rules for secure file send with Outlook Add-In, Send Portal, Reply, Drop Off, and Request File-related events.



Message Composed- Send has been pressed and basic validation done, but before Workspaces creation

Message Sent - The message is sent after the Workspace has been created.

Message Not Sent - Triggers on any error during validation and preprocessing steps

Message Viewed - Recipient visited pickup page

Message Attachment Before Download - If a download is requested, perform the Action(s) defined in this Event, then continue with downloading the attachment

Message Attachment After Download - Attachment is downloaded from the Site

Server Events

- **Service Stopped**—When the EFT service stops.
- **Service Started**—When the EFT service starts.
- **Log Rotated**—When the current activity log closes and EFT opens a new log file.

Service Stopped- Triggers if the EFT service stops.

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%

Service Started- Triggers when the EFT service starts.

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%

Type	Label (can appear in email notification)	Variable
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Site Properties	Site name	%SITE.NAME%

Log rotated - Triggers when the current activity log closes and EFT opens a new log file.

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%

Type	Label (can appear in email notification)	Variable
Source Properties (used in Copy/Move and Download Action)	Source file name without extension	%SOURCE.BASE_FILE_NAME%
	Source file name with extension	%SOURCE.FILE_NAME%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_ DIRECTORY%
	Old Log File Path	%SERVER.LOG_OLD_PATH%
	New Log File Path	%SERVER.LOG_NEW_PATH%
	Old Log File Name	%SERVER.LOG_OLD_NAME%
	New Log File Name	%SERVER.LOG_NEW_NAME%

Site Events

- **Site Stop**—When the Site stops.
- **Site Started**—When the Site starts.
- IP Added to Ban List—This Event will trigger when an IP address is banned by EFT (non-interactively) due to invalid login attempts exceeded or other security criteria.

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%
Connection Properties (for **IP Added to Ban List** event)	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Protocol	%CONNECTION.PROTOCOL%

User Events

- **GDPR Right Exercised**—The **GDPR Right Exercised** event includes an "If Event Reason [does] equal to [specific reason]" condition in the Rule Builder. This event is triggered when one of the following events are initiated:
  - When a user's personal data has been modified by someone other than the user

    or

  - Within the Web Transfer Client, when a user has:
    - Rescinded consent to the use of their personal data ("ungranted" consent to privacy policy)
    - Accessed their personal data
    - Rectified their personal data
    - Asked to restrict the use of their personal data
    - Exported their personal data
    - Objected to the use of their personal data
    - Asked to be forgotten
- **User Account Enabled**—When an administrator enables a user account on the Site. (On an Active-Active (HA) cluster configuration, add the "If node name" Condition to avoid multiple actions, such as email notifications)
- **User Account Disabled**—The user account is disabled via the Account Security settings or the Invalid login options on the user account's Security tab. This Event is also checks at midnight for any expired accounts. (On an Active-Active (HA) cluster configuration, add the "If node name" Condition to avoid multiple actions, such as email notifications)
- **User Account Locked**—The user account has been locked out by the server (for example, invalid login attempts). (On an Active-Active (HA) cluster configuration, add the "If node name" Condition to avoid multiple actions, such as email notifications)
- **User Quota Exceeded**—The user has taken too much disk space on EFT. (This applies ONLY to allotted disk space, not to file size.)
- **User Logged Out**—The user closes a session gracefully.
- **User Logged In**—The user logs in to EFT.
- **User Login Failed**—The user attempted an incorrect username or password.
- **User Password Changed**—The user or administrator changes a user's password.

- **User Account Created**—The administrator has created a new user. (On an Active-Active (HA) cluster configuration, add the "If node name" Condition to avoid multiple actions, such as email notifications)

  It is possible for a new account to be in a disabled state when the User Account Created event fires. Typically this occurs when using AD or LDAP authentication. When a synchronization occurs with the user data source, EFT creates the necessary users on the Site, but if the user is disabled in the user data source, then the new user account will be created in a disabled state. You can use the If Account Enabled Condition if the enable/disable state is part of the Action(s) you want to trigger.

- **User Account Deleted**—An administrator deletes a user account from the Site.

  User events can take these variables:

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
User Properties	(GDPR) User EU data subject status	%USER.EU_DATA_SUBJECT_STATUS%
	(GDPR) User consent to privacy policy	%USER.PP_CONSENT_STATUS%
	(GDPR) User agreement to terms of service	%USER.TOS_AGREEMENT_STATUS%
	(GDPR) Right exercised	%USER.GDPR_RIGHT_EXERCISED%
	(GDPR) Right exercised article id	%USER.GDPR_RIGHT_EXERCISED_ARTICLE_ID%
	DUNS Number	%USER.DUNS%

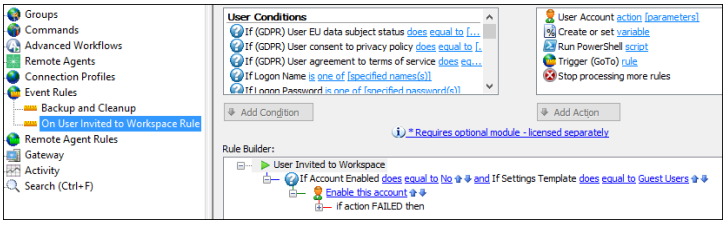
Type	Label (can appear in email notification)	Variable
	Groups	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Partner_Id	%USER.PARTNER_ID%
	Custom Field 1	%USER.CUSTOM1%
	Custom Field 2	%USER.CUSTOM2%
	Custom Field 3	%USER.CUSTOM3%
	Home Folder	%USER.HOME_FOLDER%
	Home folder is root	%USER.HOME_IS_ROOT%
	Quota Max	%USER.QUOTA_MAX%
	Quota Used	%USER.QUOTA_USED%
	Invalid login attempts	%USER.INVALID_LOGINS%
	User can change password	%USER.CAN_CHANGE_PASSWORD%
	Home IP	%USER.HOME_IP%
	User can connect using SSL	%USER.ALLOW_SSL%
	User can connect using FTP	%USER.ALLOW_FTP%
	User can connect using SFTP	%USER.ALLOW_SFTP%
	Last Login Date	%USER.LAST_LOGIN%
	Password Expiration Date	%USER.PASSWORD_EXPIRATION%
	User Must Change Password at Next Login	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
	Account Expiration Date	%USER.EXPIRATION_DATE%
	Account Locked Out	%USER.IS_LOCKED_OUT%

Type	Label (can appear in email notification)	Variable
Connection Properties	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Local Port	%CONNECTION.LOCAL_PORT%
	Protocol	%CONNECTION.PROTOCOL%
	Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
Server Properties	Server Running	%SERVER.STATUS%
	Log Type	%SERVER.LOG_TYPE%
	Log Location	%SERVER.LOG_LOCATION%
	Node Name	%SERVER.NODE_NAME%
	Install Directory	%SERVER.INSTALL_DIRECTORY%

Workspaces Events

(Requires Workspaces module) Use Workspaces Events in Event Rules if you want to be notified or cause other Actions to occur when a Workspace is create or deleted, when a use is invited to join or joins a Workspace, or when a user is removed from a Workspace. In EFT v8.5.0.8, some of the Workspaces events were renamed. The old and new names are noted below.

- **Workspace Created**- Perform actions based on a Workspace being created, such as sending an email.
- **Workspace Expired** - Perform actions based on a Workspace expiring, such as sending an email.
- **Workspace Deleted** - Perform actions based on a Workspace being deleted, such as sending an email.
- **Before Workspace Deleted/ Workspace before Delete** - Perform actions to occur before a Workspace is deleted, such as copy/move actions.
- **User Invited to Workspace/Workspace Invitation Sent** - If an account has been disabled due to expired Workspaces links, you can configure an Event Rule to re-enable the account automatically when they are sent a Workspaces invitation.



- **User Joins Workspace/Workspace Joined by User**- Perform an action when a user joins a Workspace. You could create an Event Rule using the **User Joins Workspace** Event, and add the **Email Notification Message**. In the email, you could add the variables Workspace Physical Path, Workspace Name, Workspace Participants List, and Workspace Owner. Then, whenever a user joins a Workspace, you would get an email telling you all the information you would need to know about the Workspace, including the information about the user who joined the Workspace. You could also create a custom report and define the Event Rule to generate a report automatically once per month that lists each of the Workspaces and their participants.
- **User Removed from Workspace/Workspace User Removed**- Perform actions based on a user being removed from a Workspace.

Actions

The topics below provide information regarding defining and using Event Rule Actions.

- Order in which Actions are Executed
- Available Actions
- Adding an Action to an Event Rule
- Which Actions can be Added to which Events
- Script: Advanced Workflow Action
- Cryptography: OpenPGP Configuration
- Cryptography: OpenSSL Action
- Cloud Download and Upload Actions
- Cloud: REST-Web Services Action
- Compression Action
- Export-Import to-from Dataset
- File: Operation Action
- File: Scan Action
- Flow: Abort User Operation
- Flow: Stop Processing if failed Action
- Flow: Subroutine Action
- Flow: Variable Action
- Folder: Operation Action
- Pre and Post Commands
- Loop: Dataset Action
- Datasets in Event Rules
- Protocol: Listing to Dataset Action
- Protocol: AS2 Action
- Protocol: Download Action
- Protocol: Email Action
- Creating an Email Notification Template
- Protocol Synchronize
- Protocol: Upload Action
- Example: Copying or Moving a File Triggered on Folder Monitor Event and Renamed

- Example: Send an Email Notification When a Certain User Uploads a File
- Example: Copy/Move Download File Cloud Storage Actions
- Example: Copying Folder Structure When Offloading Files
- Example: Moving an Uploaded File Based on Filename
- Smart Overwrite
- Script: Custom Command Action
- Script: PowerShell Action
- Script: Advanced Workflow Action
- System: Backup Action
- System: Cleanup Action
- System: Report Action
- Smart Overwrite
- User Action
- User Create Action
- Using Wildcards with Event Rule Actions
- Windows Event Log (WEL)

Available Actions

Once an Event Rule is triggered, assuming all Conditions are met, EFT can launch one or more of the following user-definable Actions. Some Actions require a specific module.

- Protocol: Upload(formerly "Copy/Move (push) file to host") - The designated file is automatically moved to another location.
- Protocol: Download(formerly "Download (pull) file from host") - Downloads a specified file.
- Protocol: Synchronize- Synchronize local and remote folders
- Protocol: AS2 (formerly "AS2 Send file to host" Action) - You can send files via AS2 to a partner that does not have inbound access defined in EFT's account management system.
- Protocol: Email(formerly "Send notification email") - An email message is sent to the address specified.
- Cloud: Download; Cloud: Upload (formerly Cloud Storage actions) - Supports transfers from/to Amazon S3 and Azure containers including advanced settings like multi-part, encryption, requestor-pay, and others. GET, POST, PUT, DELETE at a specific URL and save the response to a specific file.

  > **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

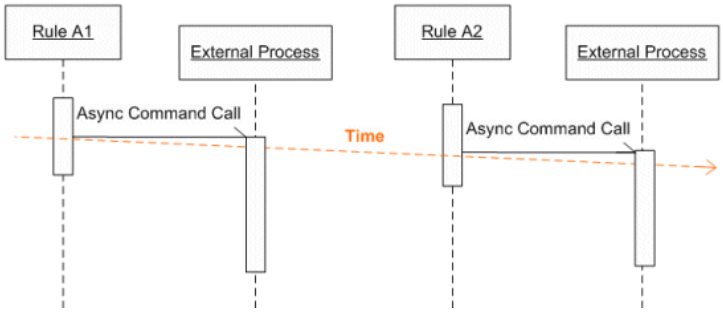
- Cloud: REST/Web Services (formerly "Invoke Web Services") - GET, POST, PUT, DELETE at a specific URL and save the response to a specific file.
- Compression - Compress or decompress file in the format of Zip, 7Zip, Gzip, Bzip2, Tar, Tar and Gzip, or ZCompress. You can also add context variables to the Action.
- Cryptography: OpenPGP (formerly "OpenPGP operations") - **(Requires OpenPGP module)**The designated cryptographic action is performed on the file.
- Cryptography: OpenSSL Action - Used to configure an OpenSSL action in an event rule to sign or verify a file.
- CSV: Export to dataset - Used in conjunction with Protocol: Listing to Dataset and Loop: Dataset Action (or with an existing dataset) to create a CSV file, which can then be used in other applications.
- CSV: Import from dataset - Reads data from a comma-separated values (CSV) file, and populates the specified dataset with those values.

- File: Scan (formerly Scan file using Content Integrity Control) - Used to send a file to an antivirus or data loss prevention scanner for processing.
- File: Operation- Create, rename, or delete specified file. Optionally use specified credentials.
- Folder: Operation- Create, rename, or delete specified folder. Optionally use specified credentials.
- Flow: Abort User Operation - Used after the File: Scan Action for a Message Composed event in case a file is attached to the message that did not pass the ICAP scan.
- Flow: Subroutine(formerly "Call Event Rule subroutine") - Allows you to call an Event Rule Subroutine event (a sub task) from the current rule
- Flow: Stop processing - If the previous trigger or Condition occurs, stop processing this Rule (default), more Rules, or this Rule and more Rules:
  - **this rule**- this Rule is not processed.
  - **more rules**- this is Rule is processed but no further Rules are processed.
  - **this and more rules** - no more Rules are processed.
- Flow: Variable(formerly "Create or set variable") - Used to create or modify a variable to be used in Event Rules
- Loop: Dataset (formerly "Loop through Dataset") - Used to read from a remote directory listing to create a dataset or read from a CSV file to create a dataset. reads through ("parses") a dataset until the end of the dataset is reached or a Loop Break is used to stop the loop.
- Script: Advanced Workflow (formerly "Execute Advanced Workflow") - An Advanced Workflow is triggered.
- Script: Custom Command (formerly "Execute command in folder") - The custom command in a specific location is triggered.
- Script PowerShell(formerly "Run PowerShell script") - Used in Event Rules to execute a PowerShell script
- System Backup- Automatically backs up EFT configuration for use in disaster recovery or EFT migration.
- System Cleanup - Cleans up a specified folder
- System: Report(formerly "Generate Report") - **(Requires database and Auditing and Reporting module)**A report is generated and emailed or saved to a file at a specific date and time.
- User: Action- Lock, disable, ban, delete, or kick user account
- User: Create - Added to an event rule when you want a certain event to trigger the creation of a new user. (This action is available to any event trigger.)

- Windows Event Log - Defines the parameters to display in the Windows Event Log when the Event is triggered.

For details of adding Actions to Rules, see the examples at the links above.

Order in which Actions are Executed



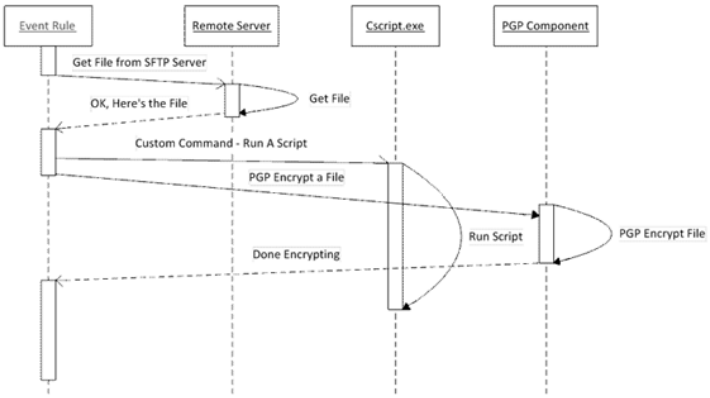
For **Execute Command** Actions and **Execute Advanced Workflow** Actions, EFT does not wait for a reply before returning control to the Event Rule thread, *unless* an "if failed" Condition is specified, such as **Stop Processing this Rule**. If an "if failed" Condition is specified, regardless of whether the Command succeeded or failed, the Event Rule processor waits for a return message from the invoked process before moving on to the next Rule.

Example: Command Action Followed by OpenPGP Action

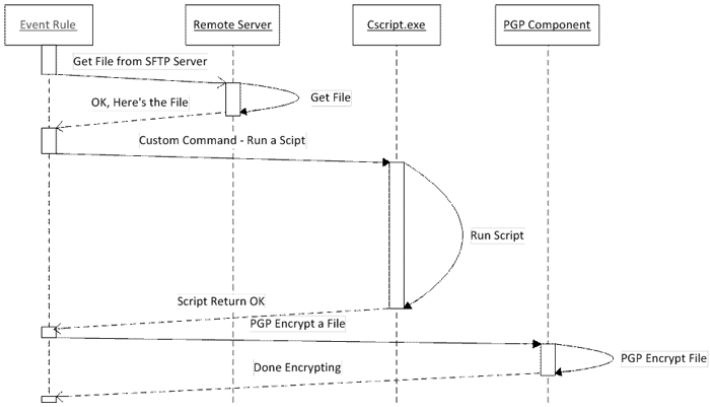
A common Event Rule scenario is downloading a file, running a script against that file (either with an **Execute Command** Action or an **Execute Advanced Workflow** Action), then encrypting or decrypting the file.

In the illustrations below, an Event Rule has three Actions: first an SFTP get (download a file from the Remote Server), followed by an **Execute Command** Action that runs a script (cscript.exe), followed by an **OpenPGP** Action.

In Example 1, an "If failed" Condition was not defined for the Command, so when the Command executes, the next Action (OpenPGP) is called almost immediately after the script is called. If you are doing a transform on the file you just retrieved that must be completed PRIOR to the OpenPGP operation, the potential risk is that there will be a race condition and likely OpenPGP will lose; that is, the pre-transformed file will be encrypted or the Action will fail because the script has locked the file for some reason.



In Example 2 we've added the "If failed" Condition so that the **OpenPGP** Action does not start until after the Command has finished running the script.



Related Topic

- Event Rule Order of Execution

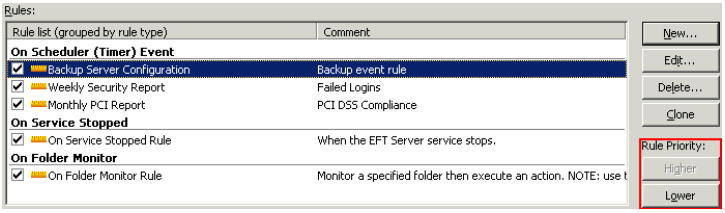
Order in which Event Rules are Executed

Almost all of EFT's Event Rule Actions are executed one after the other *(for example, execute 1, wait until it finishes, execute 2, wait until 2 finishes, execute 3 … etc.)*, because there may be Actions that follow that depend on the prior Action completing successfully. Each Action is completed before continuing to the next, with a few exceptions, which are described below (Timer Rules, Monitor Folder Rules, and Rules that use the Execute Command Action or Advanced Workflow Action).

If you create more than one Event Rule for a single type of Event trigger (for example, Monitor Folder), EFT prioritizes the Rules in the order they appear in the **Rule list**. You change the priority by moving a selected Rule up or down in the **Rule list**. The **Rule list** is grouped by Rule type. You can only prioritize the Rules within a Rule type. For example, you cannot move an **On Folder Monitor** Rule above an **On Scheduler (Timer) Event** Rule, but you can prioritize the Rules within the Rule type (for example, place one Timer Event to occur before another Timer Event).

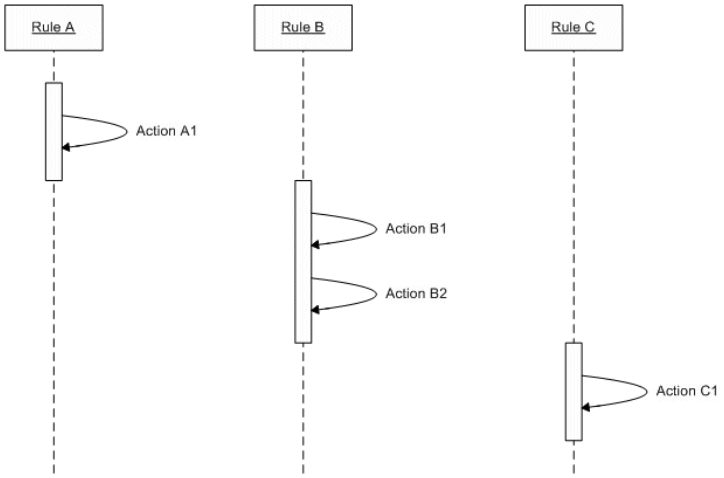
To change the priority of a Rule

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure, then click **Event Rules**. The **Rule list**appears in the right pane.
3. In the right pane, select the Event Rule you want to move.
4. To reorder the Event Rules, under **Rule Priority**, click **Higher** and **Lower**.



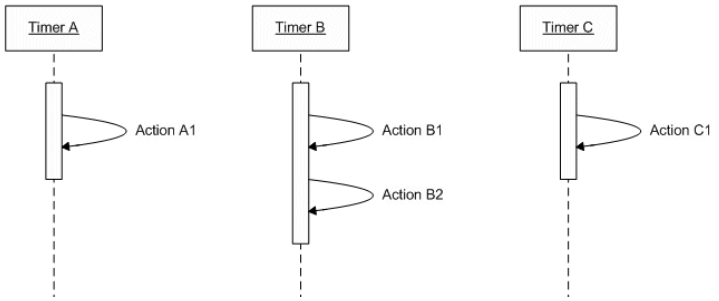
Event Rule Sequence for Matching Event Rules

One or more Event Rules may be triggered when Conditions are met. For Event Rules with duplicate Event trigger definitions and Conditions, but with different Actions, the order of execution is sequential according to the sort order defined in the interface.



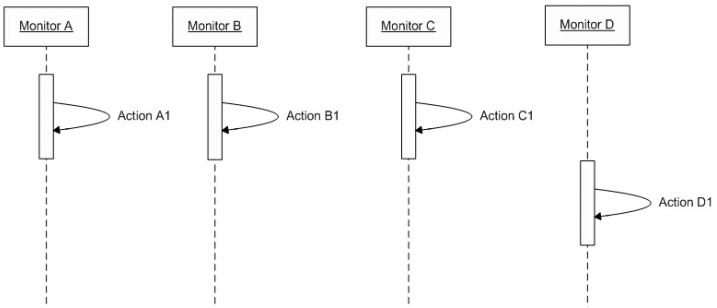
Event Rule Sequence for Matching Timer or Folder Monitor Rules

This sequential firing of duplicate Event Rules applies to almost all of EFT's supported Events. However, the Monitor Folder and Timer Event Rules are not executed at the same time. When you stop the Site or the Server service, EFT breaks all existing connections and waits until all socket threads die. The service can terminate when **Timer**Event processing is still in progress. The triggering of **Monitor Folder** and **Timer** Event Rules occurs almost simultaneously and is controlled by the operating system, not by EFT.



Event Rule Sequence for Matching Folder Monitor Rules

As mentioned above, matching **Timer**and **Monitor Folder** Events are not executed at the same time. However, **Monitor Folder** "threads" are limited to 3 concurrent threads by default. This means that if you have 5 **Monitor Folder** Event Rules monitoring the same folder and a file is added to the monitored folder, only 3 of the 5 Rules will fire, as determined by the operating system. The 4th and then 5th Rule execute only when one or more of those 3 threads are done firing and executing any actions.



Related Topics

- Condition Placement
- Order in which Actions are Executed

Adding an Action to an Event Rule

After you have created an Event Rule and added one or more Conditions (optional) to the Rule, follow the procedure below to add one or more Actions to the Rule.

To add an Action to a Rule

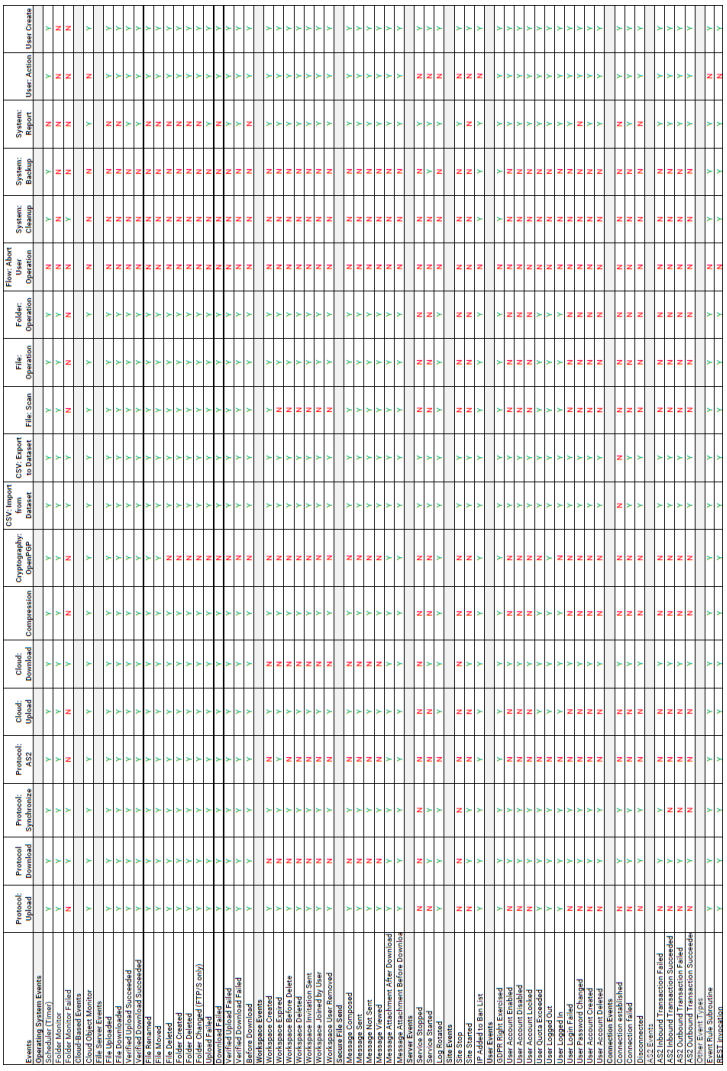
1. In the right pane, in the **Actions**list, double-click an Action or click it, and then click **Add Action**. The Action appears in the Event in the **Rule Builder**.
2. Select the linked text (blue or red) to specify parameters for the Action. For example, when you click the linked text in the **Copy** Action, the File Offload Configuration wizard appears.

Which Actions are Available with Which Event Triggers?

Some actions are only available with certain Events. The following actions can be used with any Event: Protocol: Email, Protocol: Listing to Dataset (Requires EAM), Flow: Subroutine (Requires EAM), Flow: Stop Processing, Flow: Variable, Loop: Dataset (Requires EAM), Script: Advanced Workflow (Requires AWM), Script: Custom Command (Requires EAM), Script: PowerShell (Requires EAM), and Cloud: Rest/Web Services (Requires CCM).

IMPORTANT: During the trial, all event triggers and actions are available for you to try. Any event rules that you created during the trial will no longer be available if you do not activate a license for the events and actions used in the event rules that require a license. In the EFT administration interface, event triggers and actions that require a license have an asterisk (*) next to them. Also refer to Introduction to EFT Managed File Transfer

Actions and Events Chart



Events	Protocol: Upload	Protocol: Download	Protocol: Synchronize	Protocol: AS2	Cloud: Upload	Cloud: Download	Compression	Cryptography: OpenPGP	CSV: Import from Dataset	CSV: Export to Dataset	File: Scan	File: Operation	Folder: Operation	Filter: Abort User Operation	System: Cleanup	System: Backup	System: Report	User: Action	User: Create
Operating System Events																			
Service Event	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	Y	Y
Folder Monitor	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N
Folder Monitor Failed	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N
Global Event Rules																			
Cloud Object Monitor	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	Y
Files Server Events																			
File Unlocked	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y
File Locked	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Verified Upload Succeeded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Verified Download Succeeded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
File Renamed	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
File Moved	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
File Deleted	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Folder Created	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Folder Renamed	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Folder Changed (FTP/S only)	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Upload Failed	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Download Failed	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Verified Upload Failed	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Verified Download Failed	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Before Download	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Workspace Events																			
Workspace Created	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Workspace Expired	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Workspace Failed Delete	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Workspace Deleted	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Workspace Invitation Sent	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Workspace Joined by User	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Workspace User Removed	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Secure File Send																			
Message Composed	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Message Sent	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Message Not Sent	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Message Viewed	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Message Attachment After Download	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Message Attachment Before Download	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Server Events																			
Service Stopped	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	Y
Service Paused	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	Y	N	Y	N	Y
Log Rotated	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	N	Y
Site Stop	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N	Y
Site Started	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	N	Y
IP Added to Ban List	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	Y
User Events																			
User Account Provisioned	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
User Account Enabled	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
User Account Disabled	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
User Account Locked	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
User Password Changed	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
User Logged Out	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
User Logged In	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	N	Y	Y
User Login Failed	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	N	Y	Y
User Password Changed	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	N	Y	Y
User Account Created	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	N	Y	Y
User Account Deleted	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
Connection Events																			
Connection established	N	Y	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	Y	Y
Connection failed	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	N	Y	Y
Disconnected	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	N	Y	Y
AS2 Events																			
AS2 Inbound Transaction Failed	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
AS2 Inbound Transaction Succeeded	N	Y	N	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
AS2 Outbound Transaction Failed	N	Y	N	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
AS2 Outbound Transaction Succeeded	N	Y	N	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
Other Event Types																			
Other Event Types	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y
Event Rule Schedule	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y

Cryptography: OpenPGP Configuration

The topics in chapter provide information regarding using OpenPGP with EFT.

- OpenPGP and EFT
- OpenPGP Encryption Algorithms
- Creating Key Pairs for OpenPGP
- OpenPGP KeyRing Manager
- Deleting Key Pairs for OpenPGP
- Importing and Exporting Key Pairs for OpenPGP
- OpenPGP Event Rule Action
- OpenPGP on File Upload Event Rule

See also Setting OpenPGP Security for the Site, in the **Data Security Settings section of this guide.**

In the Knowledgebase, search for PGP:
https://kb.globalscape.com/Search.aspx?Keywords=PGP

OpenPGP and EFT

EFT employs industry-standard OpenPGP (based on the open source implementation of Pretty Good Privacy) technology to safeguard data at rest. In contrast to symmetric encryption technologies that rely on a single password or shared secret for encryption and decryption, OpenPGP uses a public/private key pair and a password. Although widespread, dual-factor encryption technologies such as OpenPGP are not universally employed throughout the industry, because of the complexities involved in key creation, management, and distribution, as well as the application of public-key infrastructure technologies. Another drawback is the fact that the entire file must be present for OpenPGP encryption to work, resulting in a very brief period of time whereby data is stored "in the clear," until the encryption process is completed and the source (unprotected) file is deleted.

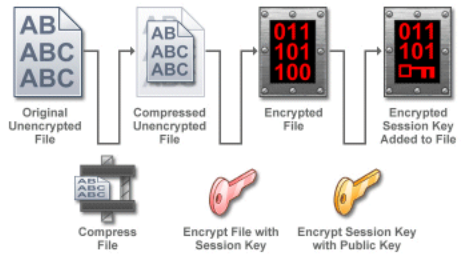
EFT supports encrypting, decrypting , signing, verifying OpenPGP messages in the format specified by RFC 4880. Refer to http://cdn.nsoftware.com/help/IG9/cs/OpenPGP.htmfor more information.

For details of using OpenPGP in Event Rules, refer to OpenPGP Encryption/Decryption Action.

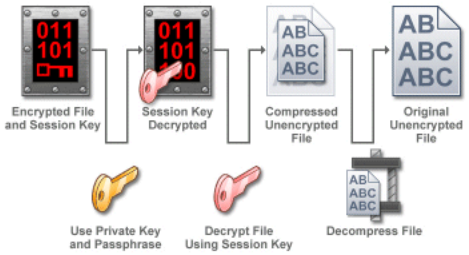
How OpenPGP Encrypt/Decrypt Works

Below are illustrations of how OpenPGP encryption and decryption works.

Encryption:



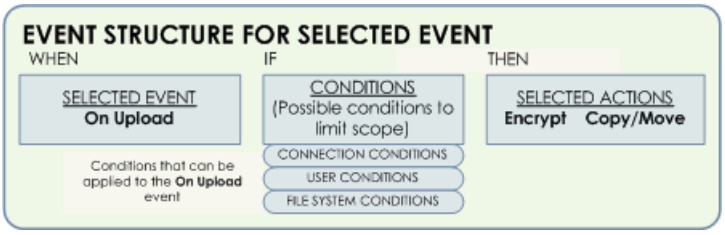
Decryption:



In EFT, the OpenPGP data encryption (or decryption) process is directed by Event Rules that specify how data files are treated in a particular context. OpenPGP uses a public key and a private key to encrypt data and maintain security. These two components are considered a key pair and are associated with a particular Site. The key pair is stored on the **OpenPGP Keyring**, which is the management tool for public keys and key pairs. The **OpenPGP Keyring** contains all key information and allows import, export, creation, and deletion of keys.

New key pairs are created using the **OpenPGP Key Generation** wizard. The wizard prompts you for key parameters and creation of a passphrase. Once the new key pair is generated, you must determine if the new key pair will be the default for the entire Site. Allowing assignment of a default key pair will automatically select this key when configuring an Event Rule using OpenPGP encryption.

The example below shows how a trigger Event (On Upload) is used to initiate OpenPGP encryption.

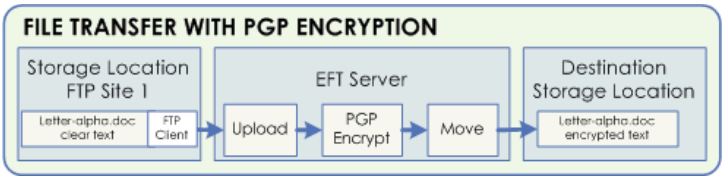


In an Event Rule, when a selected event occurs (for example, a file is uploaded to EFT), if the specified Condition exists (for example, user is member of group A), then the selected actions occur (for example, encrypt the file).

OpenPGP encryption is only available for certain Events:

- **On Upload**- when a file is uploaded to a location.
- **On Rotate Log**- when a log file is closed out and a new log initiated.
- **On Timer** - an Event that occurs once or according to a schedule.

Below is a simplified example of the file transfer process in which EFT uses OpenPGP to encrypt uploaded data and the off-load capabilities of EFT to move the file to another location.



Related Topics

- Creating Key Pairs for OpenPGP
- OpenPGP Keyring Manager
- Deleting Key Pairs for OpenPGP
- Importing and Exporting Key Pairs for OpenPGP

OpenPGP Encryption Algorithms

The table below lists the encryption algorithms available for EFT OpenPGP. It is up to you to determine which settings to use in your environment.

EFT uses IP*Works! OpenPGP libraries. Refer to EFT Specifications for the version of the library used in this version of EFT.

Ciphers – Encryption Algorithms	Message Authentication Code (MAC) – Hashing algorithms
• AES256 • AES192 • AES128 • Twofish • 3-DES • CAST 5 • IDEA	• SHA512 • SHA384 • SHA256 • MD5 • SHA1 • RIPEMD-160

Creating Key Pairs for OpenPGP

You can create new key pairs for OpenPGP encryption using the **OpenPGP Key Generation Wizard**. The key pair file is saved in **SiteConfig<GUID>.db**. Note that the **\PGP** folder does not exist until you create or import a key pair.

EFT can create the following types of keys for OpenPGP:

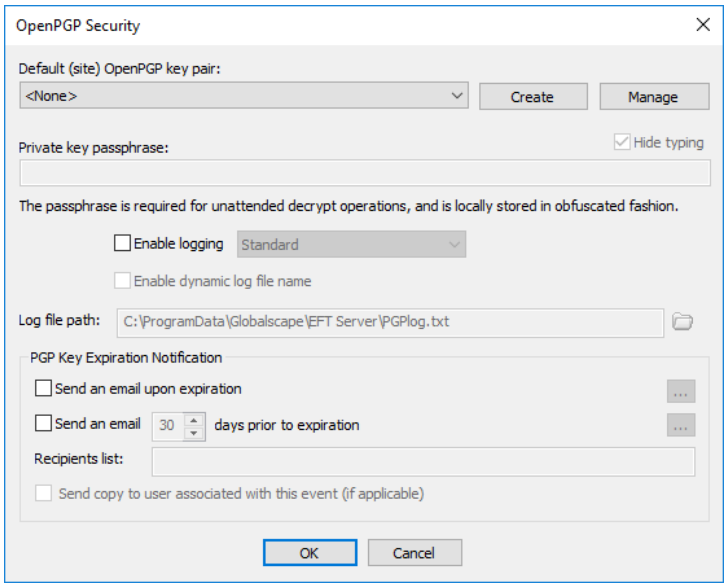
RSA: If you select RSA, the library generates the new standard RSA key pair format by default--keys that are compatible with newer OpenPGP clients. The new RSA key format supports features previously available only to DSS/DH keys. The new RSA key format enables you to have a primary key for signing and a subkey to encrypt data. In addition, the encryption key (the subkey) can be revoked or have a different expiration date as its primary key. A new subkey can always be added to a primary key and be used for encrypting data. New RSA keys are compatible with newer versions of OpenPGP. The library generates the new and improved RSA key format by default. These keys are not compatible with older OpenPGP clients that are not compliant with RFC 2440 such as OpenPGP 2.6.x.

RSA Legacy: In EFT, the OpenPGP library gives you the option to generate RSA Legacy keys that are compatible with older versions of OpenPGP. Old OpenPGP clients are compliant with RFC 1991 only, not RFC 2440.

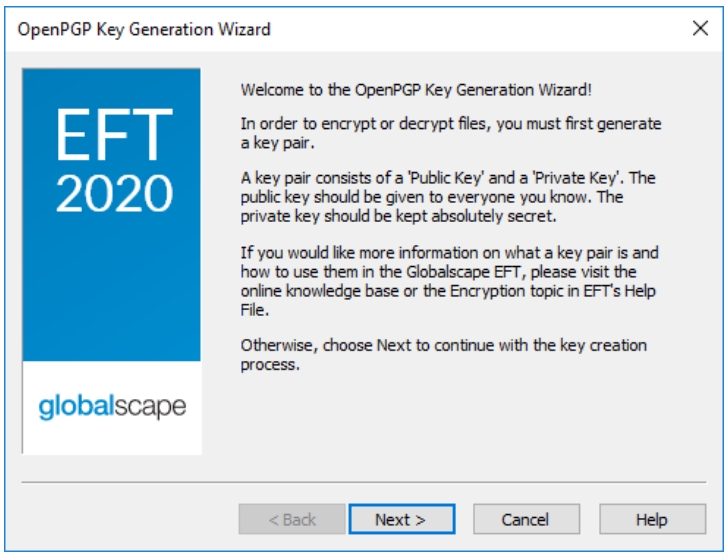
- For information about Diffie-Hellman key exchange, refer to http://en.wikipedia.org/wiki/Diffie-Hellman.
- For information about RSA, refer to http://en.wikipedia.org/wiki/RSA.
- If you have made any configuration changes, click **Apply**and/or **Refresh** before creating the key pair; otherwise, key creation will fail.
- If you attempt remote management of keys, you may encounter unexpected behavior.

To access the Key Ring Manager and use the OpenPGP Key Generation Wizard

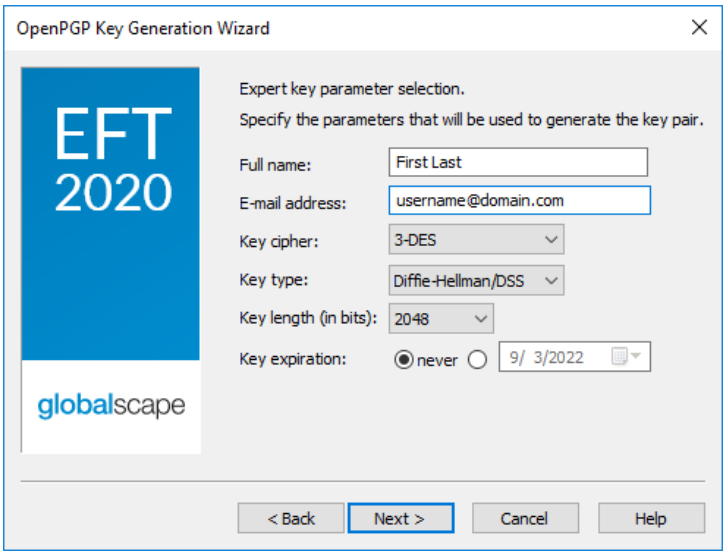
1. In the administration interface, connect to EFT and click the **Server** tab.
2. Click the Site you want to configure.
3. In the right pane, click the **Security**tab.
4. In the **Data Security** area at the bottom of the tab, next to **OpenPGP security**, click **Configure**. The **OpenPGP Security** dialog box appears.



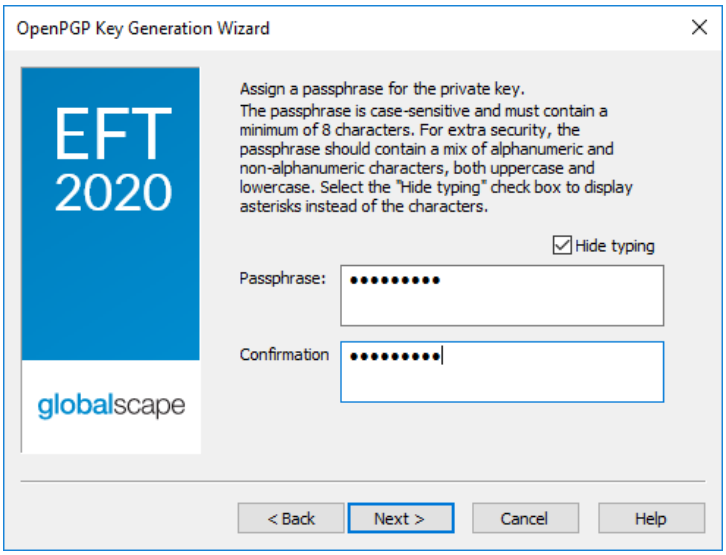
5. Click **Create**. The **OpenPGP Key Generation Wizard**appears. (Or you can click **Tools > Create OpenPGP Key**.)



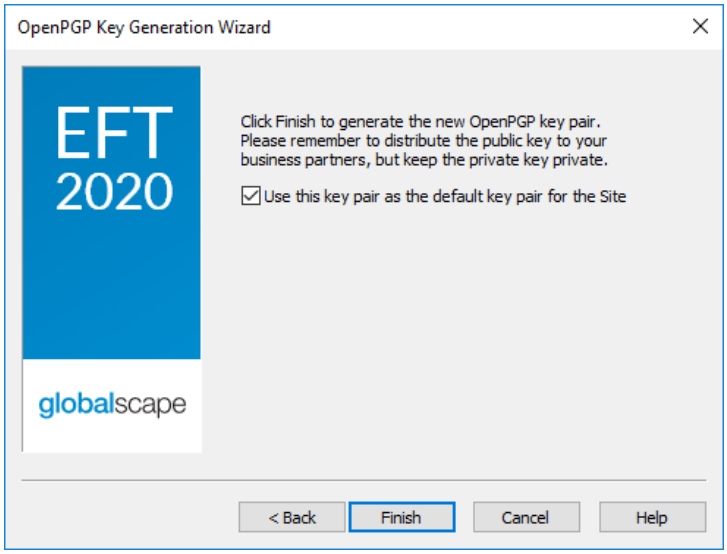
6. Read the instructions on the welcome page, and then click **Next**. The **Parameters**page appears.



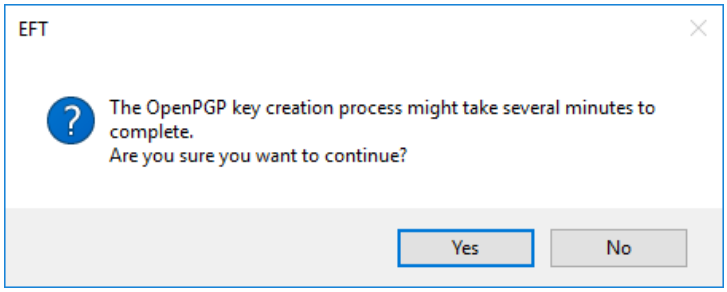
7. In the **Full name** box, provide your name or another contact's name.
8. In the **email address**box, provide an email address.
9. In the **Key cipher** box, click the list to specify a cipher to use: IDEA, 3-DES (the default), CAST5, AES128, AES192, AES256, or TWOFISH.
10. In the **Key type** box, click Diffie-Hellman/DSS, RSA, or RSA legacy.
11. Specify the **Key length**(1024, 2048, 3072, or 4096). Larger bit sizes increase security, but increase encryption time.
12. Specify the **Key expiration**date, or never.
13. Click **Next**. The passphrase page appears.



14. Type your passphrase in the **Passphrase**and **Confirmation** boxes. The passphrase is case sensitive and must contain a minimum of 8 characters. For better security, the passphrase should contain a mix of alphanumeric (both upper and lower case) and non-alphanumeric characters. Select the **Hide typing** check box to display asterisks instead of the passphrase.
15. Click **Next**. The Site page appears.



16. Click **Finish** to generate the key pair. A message appears informing you that it might take several minutes to generate the key pair.



17. Click **Yes** to create the key. If you click **No**, the key is not created.
18. After the key is created and added to the Site keyring, click **OK** to close the notification dialog box.
19. **To specify a logging Leveland the Log file path,**select the **Enable logging** check box.
20. **To specify a dynamic log file name**, select the **Enable dynamic log file name** check box, and specify an extension in the Log file path. The date and time will be added to the file name (e.g., PGPlog20190415.txt).
21. Click **OK** to save your changes and close the **OpenPGP Security**dialog box.

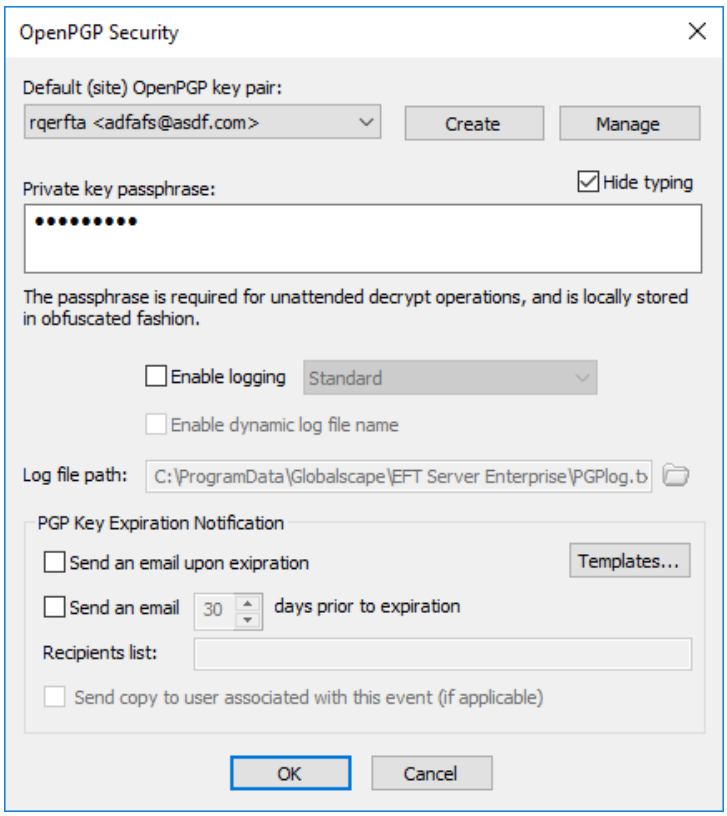
22. Click **Apply** to save the changes on EFT.

Setting OpenPGP Security for the Site

This procedure describes setting OpenPGP security for the Site.

To set OpenPGP security

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Security** tab.
4. In the **Data Security**area, next to **OpenPGP security**, click **Configure**. The **OpenPGP Security** dialog box appears.



5. If an OpenPGP key pair is defined on EFT, click the **Default Site key pair** drop-down menu and click the key. Otherwise, click **Create**and follow the instructions in Creating Key Pairs for OpenPGP or click **Manage**and following the instructions in Importing and Exporting Key Pairs for OpenPGP.
6. In the **Private key passphrase** box, provide the passphrase for the selected key. Select the **Hide typing** check box if you do not want the passphrase to be viewable.

7. Select the **Enable debug logging** check box if you want to log errors, and then click the drop-down menu to specify the level of logging: 0 (minimum logging), 1, or 2.
    - If you select the **Enable debug logging** check box, you can select the **Enable dynamic log file name** to add the date to the file name.
8. In the **Log file path** box, specify where to save the log file.
9. Under **PGP Key Expiration Notification** select the **Send an email upon expiration** check box. (EFT does a daily check at midnight.)
10. Select the **Send an email *n* days prior to expiration** check box, and specify the number of days. (The email is sent daily when nearing expiration. Acceptable values are 1 -90 days; 30 days is the default.)
11. Specify who is to receive the email. You can list multiple recipients separated by semicolons or a commas.

    The EFT log and Windows Event Viewer are updated with the same content as the template, even if email notification is disabled. The templates are stored in **C:\ProgramData\Globalscape\EFT Server\Template**s (by default). Click the buttons to the right to edit the files, if needed.

12. Click **OK** to save the changes.
13. Click **Apply** to save the changes on EFT.

Related Topics

- OpenPGP and EFT
- Creating Key Pairs for OpenPGP
- OpenPGP Keyring Manager
- Deleting Key Pairs for OpenPGP
- Importing and Exporting Key Pairs for OpenPGP

The OpenPGP Keyring Manager

Use the **OpenPGP Keyring** manager to create, delete, import, and export OpenPGP key pairs.

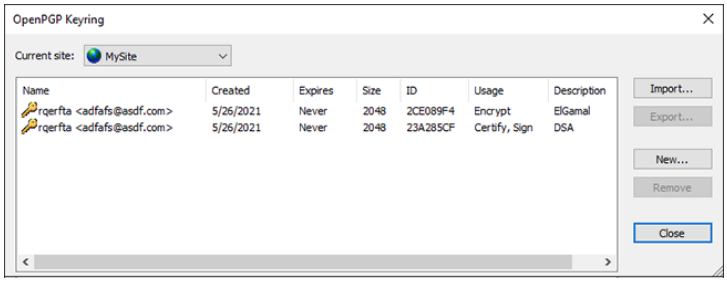
Some keys imported into EFT are dual keys: a master key used for signing, and a sub-key typically used for encrypting. When viewed in the EFT event rules PGP action, you see both keys, and it is not easy to identify which is which, as the key's email parameter is the same. EFT displays both the hex ID and that key's usage attribute (certify, sign, encrypt), to make it easier for you to choose the right key to add to the decryption set of keys.

Some PGP tools (Kleopatra, GoAnywhereOpenPGP tool suite) will display the KEY ID as a long. EFT displays the KEY ID as a short. If a KEY is imported into EFT that was created in one of these other tools, you will just see the bottom 8 hexadecimal characters in the **ID** field.

To open the OpenPGP Keyring manager

1. In the administration interface, connect to EFT.
2. Do one of the following:
   - On the toolbar, click the **Open OpenPGP Keyring**icon .
   - On the main menu, click **Tools > Manage OpenPGP Keys**.
   - On the **Server**tab, click the Site you want to configure, then in the right pane, click the **Security** tab. In the **Data Security** area, next to **OpenPGP Security**, click **Configure**. The **OpenPGP Security** dialog box appears. Click **Manage**. The **OpenPGP Keyring** manager appears.

   The **OpenPGP Keyring** manager appears.



   For each keyring, the **OpenPGP Keyring**manager displays its name, the date it was created, the expiration date, the size, a hexadecimal ID number, and a description.

   The **Current site** list displays the selected Site name.

3. For instructions for each of the features of the **OpenPGP Keyring** manager, refer to the following topics:
    - **Import**and **Export**: Importing and Exporting Key Pairs for OpenPGP
    - **New**: Creating Key Pairs for OpenPGP
    - **Remove**: Deleting Key Pairs for OpenPGP
4. Click **Close**to close the dialog box.

- After you make any configuration changes, always click **Apply**and/or **Refresh** before creating a key pair; otherwise, key creation will fail.
- If you attempt remote management of keys, you may encounter unexpected behavior.

Related Topics

- OpenPGP and EFT
- Creating Key Pairs for OpenPGP

Removing OpenPGP Key Pairs

To delete a key pair

1. Open the OpenPGP Keyring dialog box.
2. Select the key pair that you want to delete, then click **Remove**. A confirmation message appears.
3. Click **Yes**.
4. Click **Close**to exit.

Related Topics

- OpenPGP and EFT
- Creating Key Pairs for OpenPGP
- OpenPGP Keyring Manager
- Importing and Exporting Key Pairs for OpenPGP

Importing and Exporting Key Pairs

To use public key cryptography, connecting clients must have a copy of your public key. (Do not share your private key.) Export the contents of your PGP keys and store them in key files to have a backup of your keys or to share your public key with someone. You will need to import keys that you receive, or import them from storage.

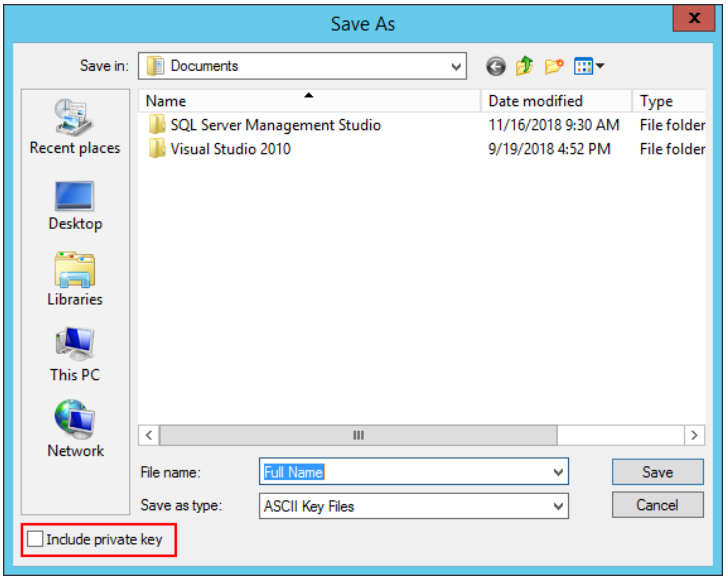
The **OpenPGP KeyRing** manager can be used to **Import** and **Export** keys. You can also sort the keyring by clicking the column headers.

To import a key

1. Open the OpenPGP Keyring dialog box.
2. Click **Import** to begin the key import process. (You can only import one key at a time.)
3. Click the file containing the key to be imported (***.asc**) then click **Open**. The **Import OpenPGP Key** dialog box closes, the imported file is added to the keyring list, the imported key is highlighted in the list, and a message box appears with the key details.
4. Click **OK** to dismiss the message box.

To export a key

1. Open the OpenPGP Keyring dialog box.
2. Select the file to be exported, and then click **Export**. The **Save As** dialog box appears.



3. Click the folder in which you want to save the new key file.

4. Select the Include private key check box to include the private key in the export. ***If you are exporting the key to provide to a client, do not select the check box.***
5. Click **Save** to export the file.

Related Topics

- OpenPGP and EFT
- Creating Key Pairs for OpenPGP
- OpenPGP Keyring Manager
- Deleting Key Pairs for OpenPGP

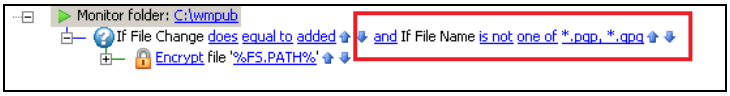
Cryptography: OpenPGP Action

You can configure EFT's OpenPGP Event Rule Action to do things like encrypt, sign, and decrypt, even on files larger than 2GB. The OpenPGP Action is available with Server Events (the **On Timer** and **On Rotate Log**events), certain File Server Events (**File Upload**, **File Move**, and **File Rename**), and a User Event (**User Logout**). To use this Action, the Site must be configuredfor OpenPGP and the appropriate OpenPGP keys must be generated.

Using the OpenPGP Action in Event Rules

When OpenPGP is used with a Folder Monitor Rule, OpenPGP operations will result in the creation of new files that will trigger the Folder Monitor Rule a second time. Although EFT provides an implicit filter that will ignore **.pgp**, **.sig**, **.asc**or **.gpg** file extensions for encrypt operations, you should still add an Event Rule Condition that provides an explicit exclusion next to the "If File Change does equal to added" Condition that is created by default when the Folder Monitor Rule is first created.

- When encrypting a file: "If File Name does not match *.pgp"
- When decrypting a file: "If File Name does match *.pgp"
- When verifying the signature: "If File Name does match *.sig"
- When signing a file "If File Name does not match *.sig'"
- When verifying signature only: "If File Name does match *.pgp"
- When signing: "If File Name does not match *.pgp"



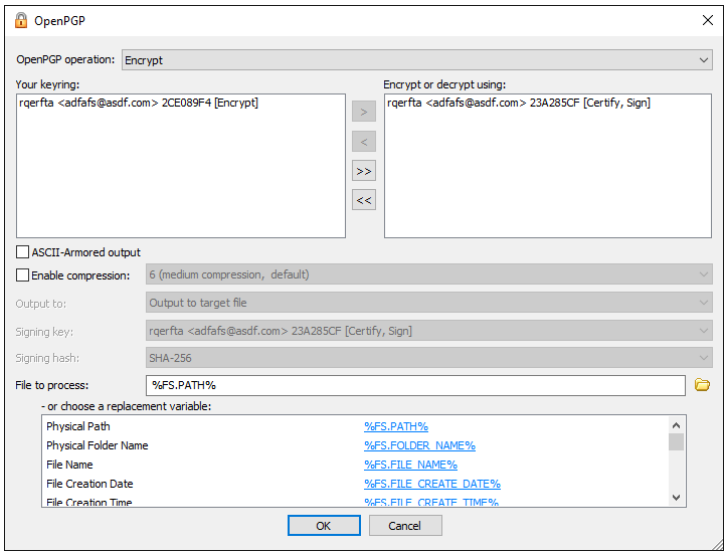
One limitation is that you cannot "Encrypt and Sign" and then "Verify Only"; that will fail. The scenarios below are valid:

OpenPGP Source	OpenPGP Receiver
Encrypt+Sign	Decrypt+Verify
Encrypt+Sign	Decrypt
Sign Only	Verify Only

To set up EFT to use OpenPGP for particular Event Rules

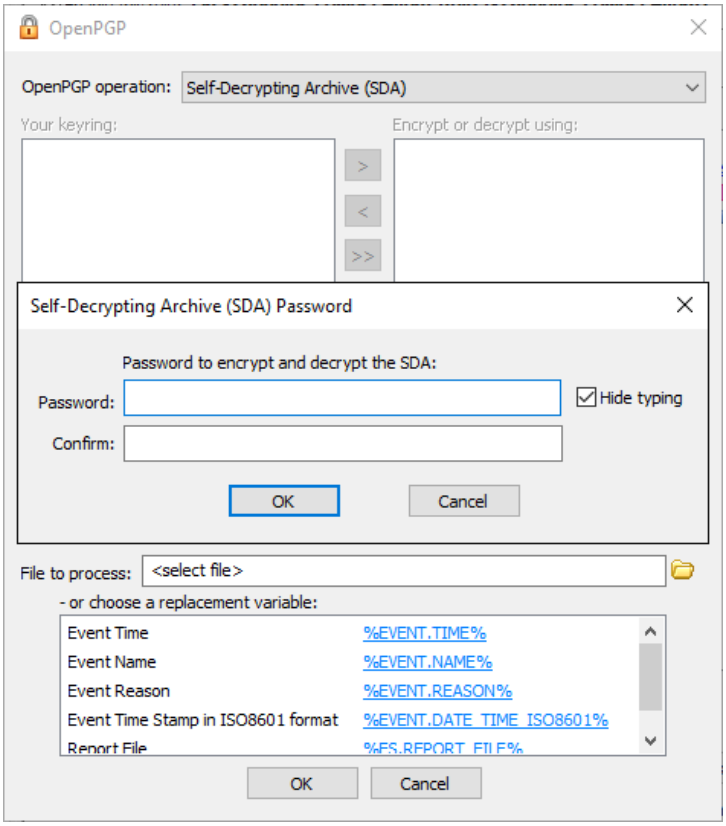
1. Follow the procedure in Creating Event Rules or select the Rule to which you want to add the Action.
2. In the right pane, in the **Actions** list, double-click **Cryptography: OpenPGP**. The Action appears in the Event in the **Rule Builder**.

3. In the **Rule Builder**, select either of the underlined elements (links). The **OpenPGP** dialog box appears.



4. Specify the **OpenPGP operation** (Encrypt, Encrypt and Sign, Sign Only, Self-Decrypting Archive (SDA), Decrypt, Decrypt and Verify Signature, Verify Signature Only).

   When **Self-Decrypting Archive** is selected, none of the encryption settings are available. The SDA Class uses a Deflate algorithm specified in RFC 1951for compression, and then creates a self-decrypting executable archive. It doesn't use encryption in the standard sense like AES, etc. Therefore, it is not considered secure when matched up against OpenPGP. After you click **OK**, a password dialog box appears. Create and confirm a password, click **OK**, then send the password to the recipient. Use a different OpenPGP operation if you want to use encryption.



5. The options that appear in the dialog box depend on what you select in the **OpenPGP operation**box:
    a. If you designated a default key for the Site, that key is displayed in the **Encrypt or decrypt using** (right) pane. If there is no default key, the right pane will be blank. Use the arrow icons to add or remove keys between the **Your keyring** pane and the **Encrypt or decrypt using** pane, or double-click the key in the list.

    If you would like to encrypt a single file such that multiple recipients will be capable of decrypting it, add the individual keys of the intended recipients to the list of keys to use for the encryption Action to the **Encrypt or decrypt using** (right) pane. This prevents you from having to create multiple copies of a file and then encrypt and manage each file separately for each intended recipient.

    Example Use Cases:

    - You have a report containing sensitive data in PDF format. You want to encrypt and send that report to three people. In this case you would configure the "Encrypt" or "Encrypt and Sign" Action with all three public keys that correspond to those individuals. You can then send a copy of that one file to each of the recipients, and they can

each decrypt the file with their private key in order to view the report in their PDF reader.

- You are required to keep an archived copy of all outbound files, including any encrypted files. If you encrypt with only the intended recipient's key, then the resulting encrypted file will not be acceptable for archival since you will not be able to decrypt it later. Therefore, you encrypt the file with not only the public key of the intended recipient but also the public key to which you have the corresponding private key. Not only will the recipient be able to decrypt the file as usual, but you will also be able to decrypt the archived copy of that file, if needed.

b. To specify **ASCII-Armored output**, select the check box.

c. Select the **Enable compression** check box, and then click the down arrow to specify a level of compression, from 1 (least compression, fastest) to 9 (max compression, slowest). The default is 6 (medium compression, default).

d. In the **Output To** box, click the down arrow to specify an option: Output signature to target file (.pgp), Output signature to target file ASCII armored (*asc), Output signature to separate file (*.sig), Output signature to separate file ASCII armored (*.asc).

e. In the **Signing key** box, click the down arrow to specify the signing key.

f. In the **Signing hash** box, click the down arrow to specify a hash: Use default (MD5 or SHA-256), MD5, SHA-1, RIPEMD160, SHA-256, SHA-384, or SHA-1512. The default value depends on the version of the key used to sign the message. For version 3 keys (RSA Legacy keys), MD5 is used as default value. For all other keys, SHA-256 is used. The encryption method and compression method are both chosen by the ciphers that are used/chosen when the key was created. These ciphers are stored in the metadata of the key. EFT reads this metadata and uses that cipher for encryption/compression process.

g. In the **File to process** box, specify the file or folder to process. The default target file is selected. Alternatively, click a variable to add it to the **File to process**box or use actual file/folder names. Use the folder icon to browse to a file or folder.

IMPORTANT: If the event rule is configured to encrypt or decrypt a file located on a network share, the EFT service account will need full access to the location where this file is located, unless the event rule being used is providing alternate credentials that have full access to the file(s).

6. Click **OK** to close the dialog box and apply the parameters.

7. Click **Apply**to save the changes on EFT.

OpenPGP on File Upload Event Rule

For this example, we will create an Event Rule to trigger when a file is uploaded to the destination folder of the Folder Monitor Rule.

We want this Event Rule to decrypt the uploaded encrypted file, then:

- If the Action failed to decrypt the file, then:
  a. Send email notification, and
  b. Write to Windows Event Log.

Prerequisites

- Private OpenPGP key (part of original key pair)
- Email address for notification

To create a File Upload Event Rule

1. Create a new Rule.
2. Select the File Uploaded event trigger and name the Rule.
3. Add the **File Name** Condition to the Rule.
4. Configure the **File Name** Condition to trigger only on files with the PGP extension.
5. Add the **Cryptography: OpenPGP** Action.
6. Set the OpenPGP action to **Decrypt**. (Only private keys added to the keyring will show in the list when choosing to decrypt.)
7. Add the **Protocol: Email** Action under the **if action failed** Condition.
8. Configure the email as desired.
9. Add the Windows Event Log Action, and specify which variables to write to the Event Log, such as the file name.
10. Click **Apply** to save the Event Rule.

Cryptography: OpenSSL Action

You can configure an OpenSSL action in an event rule to sign or verify a file.

The OpenSSL action is supported on HTTPS and SFTP and can be used for the following triggers:

- Scheduler (Timer)
- Folder monitor
- File Uploaded
- Verified Upload Succeeded events

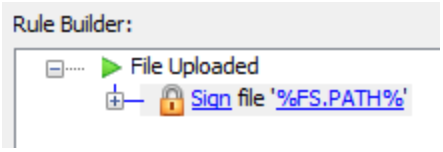
EFT can only create detached signature files; however, it can verify signatures for non-detached, detached, and XML Enveloped signature files.

The signing certificate formats include:

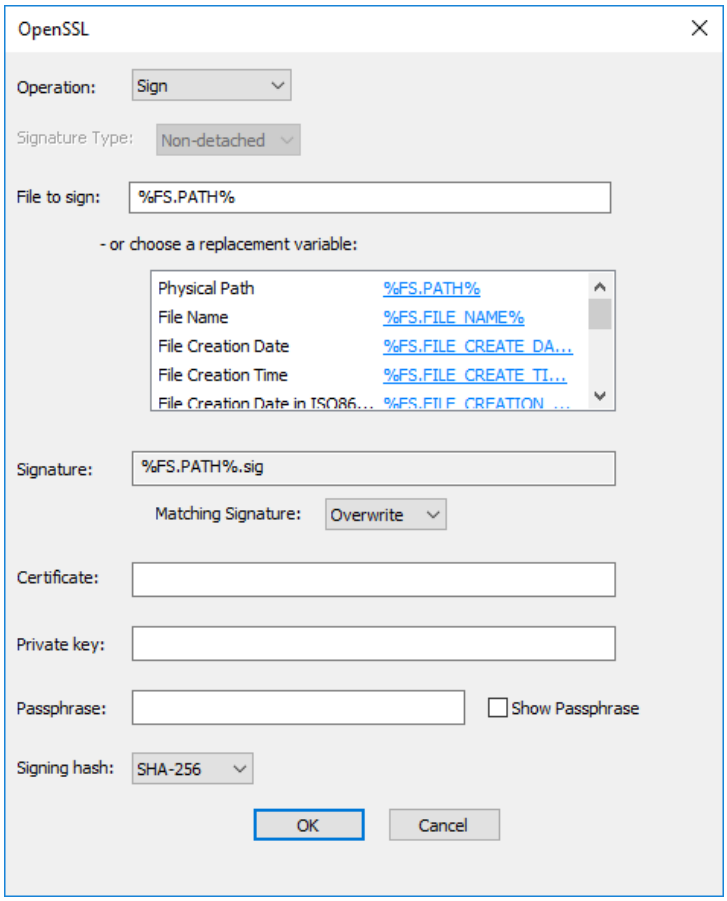
- .pem
- .cer, .crt, .der – in binary DER form only
- .p7b, .p7c – PKCS#7 SignedData structure without any data, just the certificate
- .p12 – PKCS#12, may contain certificate(s) (public) and private keys (password protected)
- .pfx – PFX, predecessor of PKCS#12 (usually contains data in PKCS#12 format, e.g., with PFX files generated in IIS)

To use the Cryptography: OpenSSL action

1. Create an event rule (or use existing rule) and add the action to the event.



2. Click one of the linked items. The **Open SSL** dialog box appears.



3. In **Operation**, click the drop-down list and click **Sign** or **Verify Signature**. The available fields change depending on whether you choose **Sign** or **Verify Signature**.
4. If you clicked **Sign**, the **Signature Type** field is read-only.

> **NOTE:** EFT can only create detached signature files, however, it can *verify* signatures for non-detached, detached, and XML-Enveloped signature files.

- In the **File to sign** box, The File System variable %FS.PATH% is the default. You can chooses a replacement variable instead.
- The **Signature** field is read-only and displays the filename of the signature file path used, which is the same as the file to process, with ".sig" appended to the filename. This text box is auto-filled and non-editable.
- In **Matching Signature**, specify what to do if a duplicate signature is found: **Overwrite**, **Skip**, or **Fail**.
- In the **Certificate**, **Private Key**, and **Passphrase** fields, provide the associated certificate information.

> **NOTE:** You cannot browse for the certificate or private key location. Instead you must copy and paste the path to the certificate and private key. EFT server must have access to the location.

- The **Show Passphrase** check box allows you to verify the passphrase was typed correctly.
- In **Signing hash**, click the applicable algorithm: **SHA-256**, **SHA-384**, **SHA-512**.

5. If you clicked **Verify Signature**, in **File to sign**, specify the file path, or click another variable in the list of replacement variables. Then specify the **Certificate** path and click **OK**.
6. Add additional actions or conditions as needed, then click **Apply** to save the Event Rule.

> **NOTE:** A context variable, EVENT.EVENT_ACTION_FAILURE_REASON, can be used to convey error information returned from the OpenSSL library to any downstream actions.

Cloud Download and Upload Actions

Cloud storage actions are used in Event Rules to copy and move files to cloud storage and/or download files from cloud storage. Clicking the cloud storage link in those actions allows you to specify the storage. When you use a Cloud Object Monitor event, the **Cloud: Download** action is added automatically. Then you can add the **Cloud: Upload** action (or other actions).

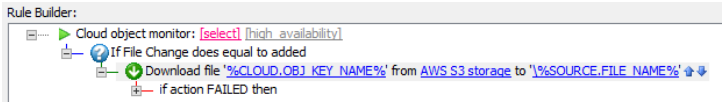
> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

These instructions assume you have already created your cloud storage and know the connection details to provide to EFT. It is recommended that you configure your cloud connector first in a Connection Profile.

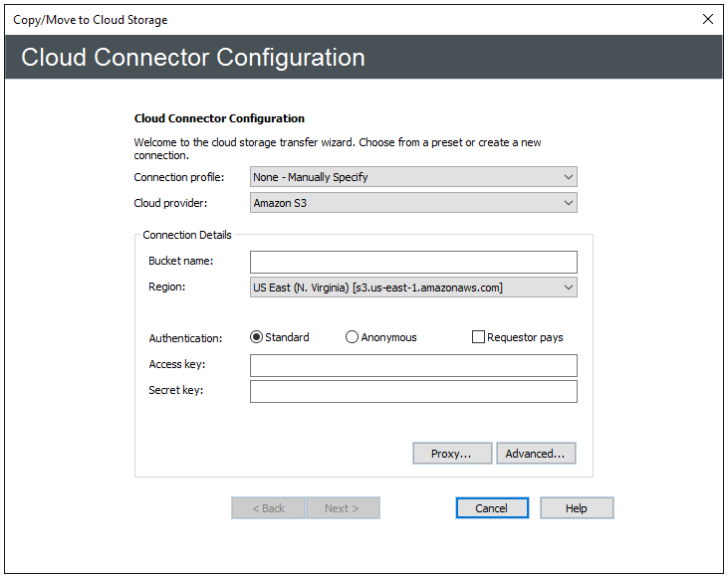
> **NOTE:** Do not confuse cloud Actions with the File Transfer module, which provides copy, move, upload, and download from non-cloud storage.

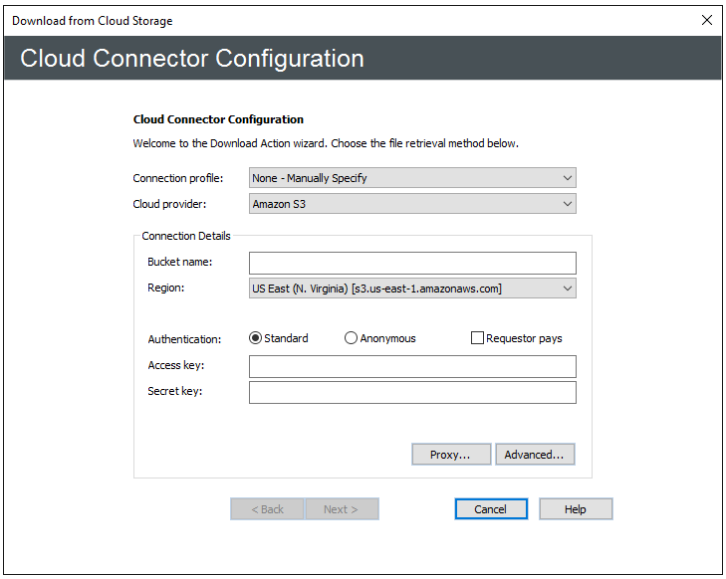
For Upload and Download actions, configure the Rule as described below

1. Follow the procedure in Defining Event Rules to add an event to the Rule Builder and then add the **Cloud: Download** or **Cloud: Upload** Action.



2. In the Rule Builder, click in the **Cloud: Download or Cloud: Upload** action. The configuration wizard appears.





3. In the **Copy/Move** and **Download** wizards, configure the **Cloud Connector Configuration** page to specify the cloud provider storage and other details, based on which cloud provider you specify. (You could configure a cloud provider in a Connection profile to avoid having to configure connection details for every Event Rule. Refer to Defining a Connection Profile for details of connecting to cloud storage.)
4. In the **Source Object** page of the wizard, specify the source **Object name**. You can specify file names, paths, or context variables, and specify whether to **Delete object file after it is downloaded** and **If the source file is missing, treat as success**.

   > **NOTE:** You cannot browse for files in cloud storage.
   > In the **Cloud: Download Action** wizard (**Download from Cloud Storage**) on the **Source Object** page, the browse button in the **Object name** field is not available.
   > In the **Cloud: Upload Action** wizard (**Copy/Move to Cloud Storage**) on the **Destination** page, the browse button in the **Object name** field is not available.

5. Specify the **Destination path** for folder and filename (optional). Context variables can be used here also. You can also specify what to do with **Matching filenames** (**Overwrite**, **Skip**, or **Numerate**) and **Rename transferred file**.

Refer to the following topics for information about creating EFT Event Rules:

- Defining a Connection Profile
- Introduction to Event Rules

- Defining Event Rules
- Advanced Transfer Options

Cloud: REST-Web Services Action

(Requires CCM) The **Invoke Web Service from URL** Action can be used to integrate with an external server or application, such as auditing external systems.

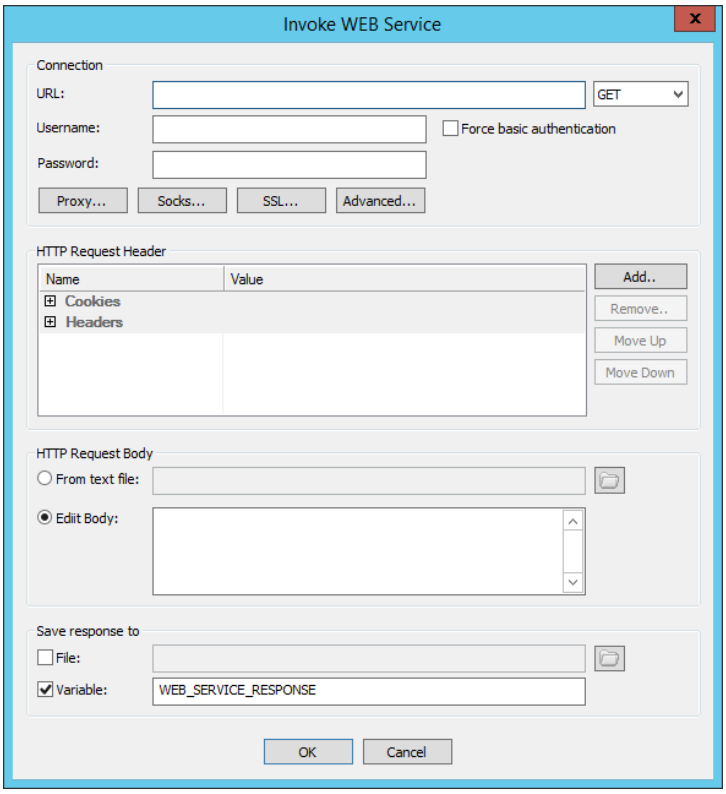
Refer to EFT Web Service for information about enabling the Web service in EFT.

The Web Service allows you to initiate an Event Rule from an external application, such as an enterprise scheduler. After the Event Rule finishes dispatching, the Web service responds with an XML document that consists of a single "Result" element. Adding an advanced property/ registry setting described in the Knowledgebase article linked below will modify the original response to add context variables that are in the XML document, from which you can then parse out values with another application.

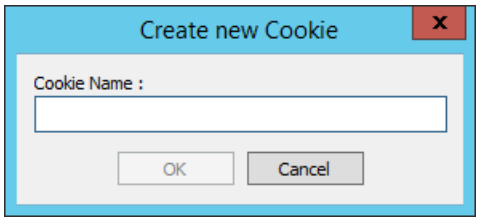
https://kb.globalscape.com/Knowledgebase/11441/Add-Context-Variables-and-Values-to-Web-Services-XML-Response

To define the Invoke Web Service Action

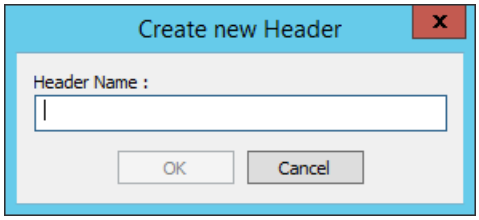
1. Add the Event to the Event Rule (for example, File Downloaded).
2. Add any (optional) Conditions.
3. Add the **Cloud: REST-Web Services** Action.
4. Click any links in the Action to open the **Cloud: REST-Web Services** dialog box.



5. In the **URL**box, provide the URL on which to perform the **Invoke Web Service** Action.
6. Select the drop-down list to specify **GET**, **POST**, **PUT**, or **DELETE**.
7. In the **Username**and **Password** boxes, provide the credentials needed to log in to the URL.
    - Select the **Force basic authentication** check box, if needed.
8. (Optional) If you connect to the URL through a proxy server, click **Proxy** and then specify the **Proxy type**, **Host name**, **Port**, **Username**, and **Password**. Refer to Proxy Settings Dialog Boxfor details.
9. (Optional) To specify an **Authentication Type** and login sequence, in the **Proxy Settings** dialog box, click **Advanced**. The **Advanced Proxy Settings**dialog box appears. Refer to Advanced Transfer Options for details.
10. (Optional) If you connect to the URL through a Socks server, click **SOCKS**. Refer to Using a SOCKS Proxy Serverfor details.
11. (Optional) If you chose a protocol that uses SSL (**FTPS** or **HTTPS**), provide the client and remote server's SSL certificate information. Refer to SSL Options Dialog Box for details.
12. In the **Invoke Web Service** dialog box, in the **HTTP Request Header** area, do the following:
    - Click **Cookies**, then click **Add** to create a new cookie, provide a name for the cookie, then click **OK**.



    - Click **Headers**, then click **Add** to create a new header, provide a name for the header, then click **OK**.



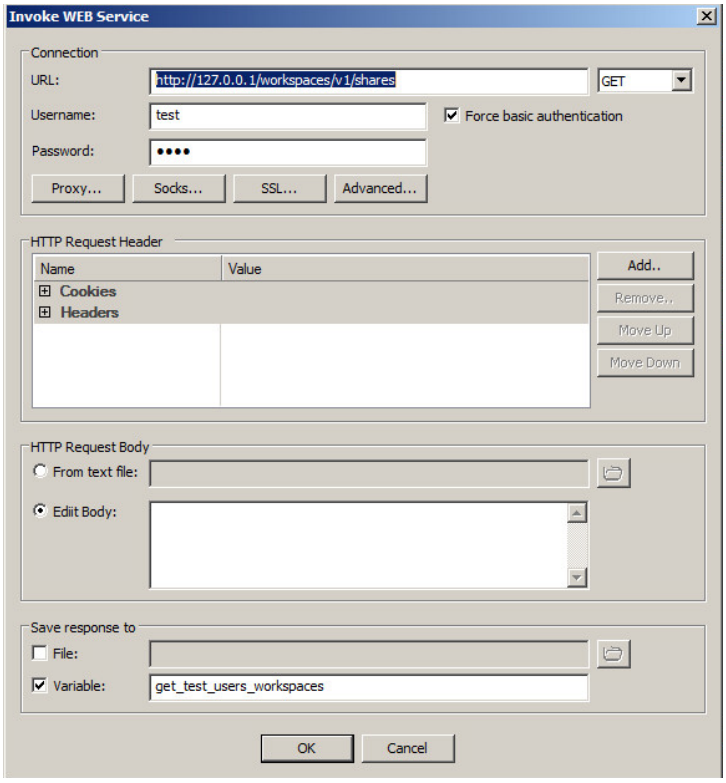
13. In the **HTTP Request Body** area, do one of the following:
14. Select **From text**file, then specify the text file from which to use the text.
15. Select **Edit Body**, then specify the text to use in the body of the HTTP Request.
16. In the **Save response to** area:

- Select the **File**check box, then specify the name and path to the file, or click the folder icon to specify it.
- Select the **Variable**check box, then specify the variable in the box. This variable can be anything you want, to be used in other places, such as the Windows Event Log.

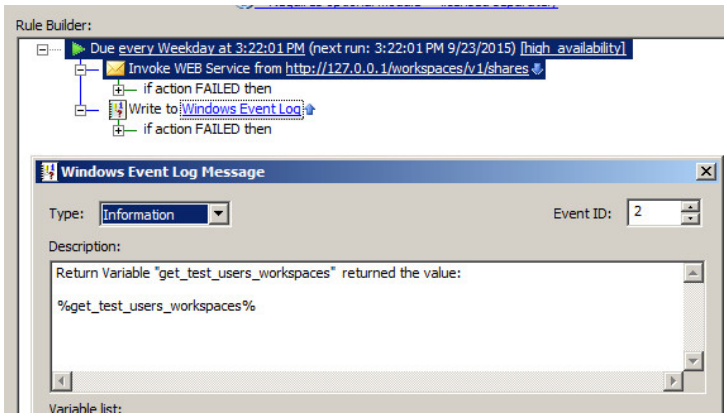
17. Click **OK**.

Example:

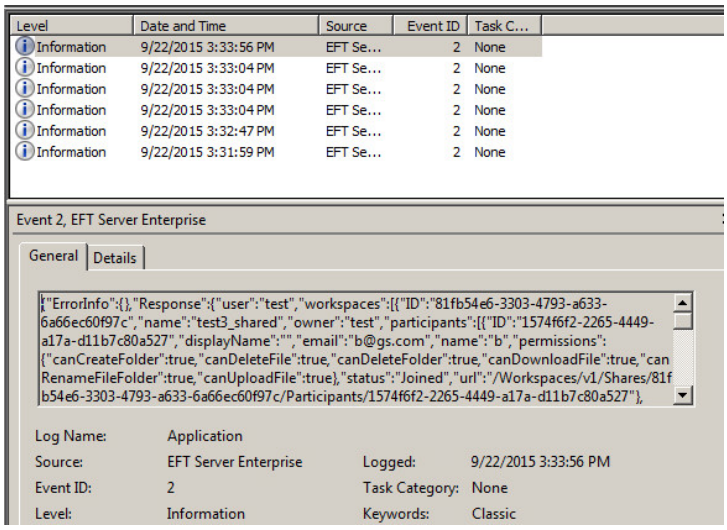
Below, the default value of `WEB_SERVICE_RESPONSE`is changed to `get_test_users_workspaces`.



You can use this variable within the same Event Rule call, such as to write to the Windows Event Log:



As shown below, when the Event is triggered, the Log reports the value of the response variable `get_test_users_workspaces`.



Azure Data Lake Storage

Azure Data Lake Storage is a highly scalable and cost-effective data lake solution for big data analytics. Data Lake Storage Gen2 extends Azure Blob Storage capabilities and is optimized for analytics workloads. EFT Event Rules allow you to store files in or monitor for added files in Azure's Data Lake generation 2 (ADLSg2), so that you can reduce cost when compared with saving files into a standard blob storage.

Containers created with ADLSg2 support can be monitored by a Folder Monitor Event as long as the Azure container credentials and Active Directory domain trust relationship is enabled.

To use a Folder Monitor Event to monitor an Azure file share, be sure to enable the VFS overrideand create a virtual folder that points to the Azure file share path.

EFT Secrets Primer (Knowledgebase)

From https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-introduction:

The following are the equivalent entities, as described by different concepts. Unless specified otherwise these entities are directly *synonymous*:

Concept	Top Level Organization	Lower Level Organization	Data Container
Blobs – General purpose object storage	Container	Virtual directory (SDK only – does not provide atomic manipulation)	Blob
Azure Data Lake Storage Gen2 – Analytics Storage	Container	Directory	File

Related Topics

- Configuring Azure Key Vault Support for EFT
- Configuring the Secrets Module
- Override VFS Credentials
- Folder Monitor Event

EFT Web Service

The Web Service allows administrators to initiate EFT workflow from an external application such as an enterprise scheduler. The WebService interface follows the model of ASP.NET Web services, providing a page for the services definition document (WSDL) and an HTML form that can be used to test available service methods. (Download and use the Web Service scripts to test the Web Service with Powershell.)

The procedures below provide instructions to:

Enable the Web Service in EFT

Use the Invoke Web Service Action

- Access to Web Service requires authentication with a COM-enabled Server administrator account; without proper authentication and COM privileges, EFT returns a `401 Unauthorized HTTP error` to the requestor.
- An SSL certificate is required to use Web Service, because EFT sends the HTTP Web Services requests via HTTPS. (Specify SSL versions and ciphers before enabling SSL connections. SSL must first be enabled on EFT and the Site.)
- The Web Service is enabled in the Site's **Listener Settings** area. EFT allows you to turn on Web Service without selecting the **HTTPS**check box, but it checks for an SSL certificate, because it will automatically redirect HTTP to HTTPS. Even when the **HTTPS** check box is not selected, Web Service requests are handled by the HTTPS engine (port 443 listener, by default), but other HTTPS requests will still get the 503 Service unavailable response.
- EFT uses a template for the WSDL to construct the final WSDL. External tools can use the WSDL by pointing to the URL that deploys the WSDL file at
- **http://localhost/WebService/InvokeEventRule?wsdl**, where "localhost" is the IP address, computer name, or DNS name that points to the EFT service that is hosting the web service.
- Requests to any /WebService URL is logged to the text log and ARM system just as any other HTTP request.
- The Web Service timeout is set to 60 seconds. You can change the timeout value with the advanced property described in https://kb.globalscape.com/KnowledgebaseArticle10553.aspx.

Requests to any **/WebService**URL are logged to the text log and ARM database just as any other HTTP request. A request that does not match the **/WebService/InvokeEventRule**URL or that does not include the required parameters, results in a `400 Bad Request HTTP error`.

The **/WebService** page displays a list of Web services available with EFT. This page is generated from an HTML page in EFT installation folder, in a subfolder called **WebService**.

By default, the following files are installed in: **C:\Program Files\Globalscape\EFT Server\Web\WebServices**

- **\EFTWebServices_MAIN.html**- Used to define the Web Services landing page; provides a link to **InvokeEventRule.html**.
- **\InvokeEventRule\EFTWebServices_InvokeEventRule.html**- Used to define the Web interface from which you can remotely invoke Event Rules on EFT.
- **\InvokeEventRule\EFTWebServices.wsdl**- Web Services Description Language (WSDL) configuration file. (For details of how WSDL files are used, refer to the World Wide Web Consortium documentation at http://www.w3.org/TR/wsdl.)

How EFT Supports the Web Service

EFT supports both POST and GET HTTP requests to "/WebService/InvokeEventRule" with two parameters "EventRuleName" and "EventParams" and triggers an Event Rule that is specified in the "EventName." The Web Service supports the REST invocation model, supporting both POST and GET methods for invocation.

1. If an input is missing any of "EventRuleName" or "EventParams" it returns an HTTP 400 error.
2. If both "EventRuleName" and "EventParams" are presented but:
    a. "EventRuleName" is wrong (no Event Rule exists with such name), it returns .xml with result code of -1.
    b. "EventParams" are incorrect (wrong variable names, too many, too few), EFT looks for Rule variables in the input and replaces those values with found ones. All additional variables are ignored. If a Rule variable is not found in URL then it will be set to "N/A." The result code in .xml will be the Event execution result code.

HTTP GET

The following is a sample HTTP GET request and response. Replace the placeholders with values.

```
GET /WebService/InvokeEventRule?EventRuleName=string&
EventParams=string HTTP/1.1 Host: localhost

HTTP/1.1 200 OK Content-Type: text/xml; charset=utf-8
```

```
Content-Length: length <?xml version="1.0" encoding="utf-8"?>
<int xmlns="http://mydomain/">int<int>
```

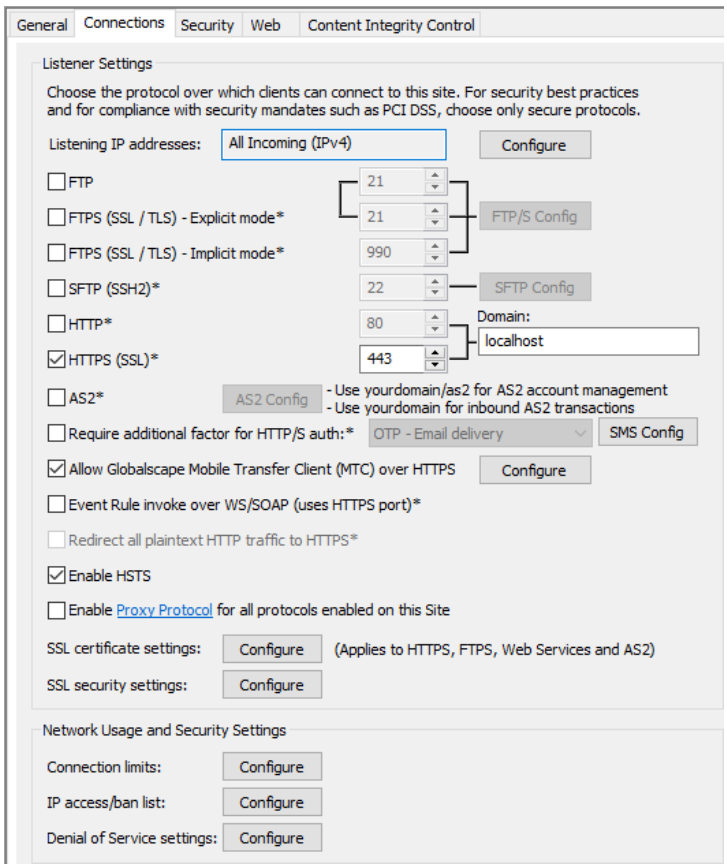
HTTP POST

The following is a sample HTTP POST request and response. Replace the placeholders with values.

```
POST /WebService/InvokeEventRule HTTP/1.1 Host: localhost
Content-Type: application/x-www-form-urlencoded Content-Length:
length EventRuleName=string&EventParams=string

HTTP/1.1 200 OK Content-Type: text/xml; charset=utf-8
Content-Length: length <?xml version="1.0" encoding="utf-8"?>
<int xmlns="http://mudomain/ ">int</int>
```

To enable the Web service in EFT

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site that you want to configure.
3. In the right pane, click the **Connections** tab.



4. Select the **Event Rule invoke over WS/SOAP (uses HTTPS port)** check box.

   IMPORTANT: If this is not enabled, you will not be able to log in to the Web Service.

5. Click **Apply** to save the changes on EFT.

To use the scripts for testing Web Service

Use one of the attached scripts to test Web Service (copy into PowerShell).

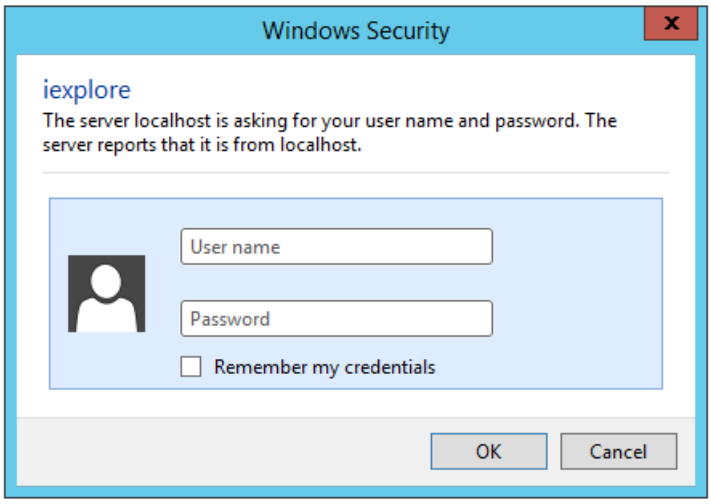
- **EFT.InvokeEventRule.ps1** uses regular output -1, 0 or 1 (classic SOAP)
  - Change the various strings at the top for host, administrator username, password, and event rule name.
- **InvokeEventRule.ps1** returns all context variables from the rule (behaves a bit more REST like, even though the response is XML, not json).
  - Add the advanced property "EventWebServiceResponseAddContextVariables" to the AdvancedProperties.JSON file. You must set this property to get the payload from EFT in response showing the context variables.
  - Change the administrator username and password various strings at the top of the script.
  - Modify the Invoke-WebRequest method, including the host, event rule name, and optional parameters.

To execute an Event Rule using Web Service

1. Open a browser and navigate to EFT URL appended with `/WebService`. The **WebService** page appears.

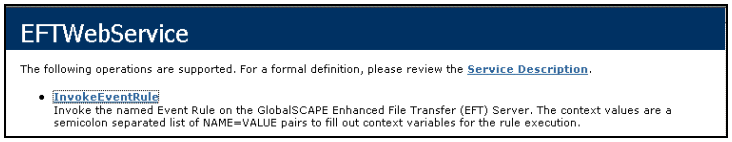
   IMPORTANT: You must change the URL of the Site and the port number if you are not using "localhost" and port 443, as shown below!

2. A login prompt appears. Provide a COM-enabled Server administrator account login credentials. If the **Event Rule invoke over WS/SOAP (uses HTTPS port)** check box is not enabled on the Connections tab of the Site, you will not be able to log in to the Web Service.

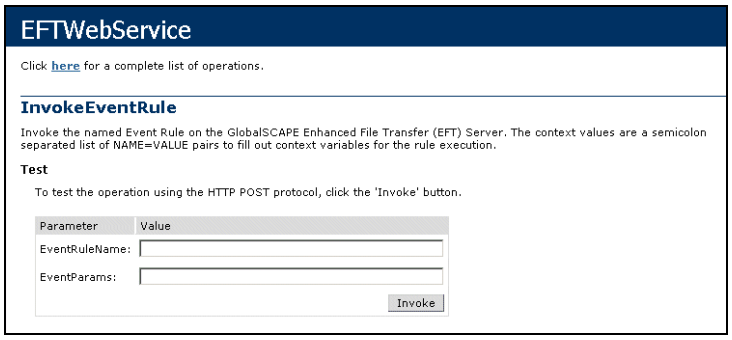


IMPORTANT: EFT leverages the USER https port (443 by default); however, WebService uses the Server administrator accountlogin credentials, not USER credentials!

3. The EFTWebService interface appears.



4. Click **InvokeEventRule.**Another Web page, **/WebService/InvokeEventRule**, displays a form for invoking an Event Rule.



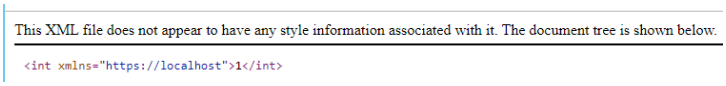
5. In the **EventRuleName**box, type the name of the Event Rule.
6. In the **EventParams**box, type one or more variables, separated by semicolons.
7. Click **Invoke**. The Event Rule is executed.

   All WebService responses use the Site's domain name as the namespace for the WebService.

   For example, in the **EventRuleNameValue** box, type `Backup and Cleanup`. Leave **EventParams**blank, and then click **Invoke**. The browser returns the following string:

```
<int xmlns="HTTPS://localhost:443/">1</int>
```

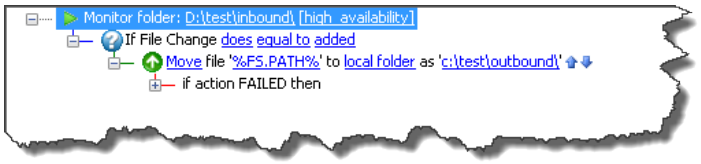
- 0 indicates failure
- 1 indicates success
- -1 indicates EFT could not find the Event Rule (for example, the requested EventName does not exist or was not typed correctly.)

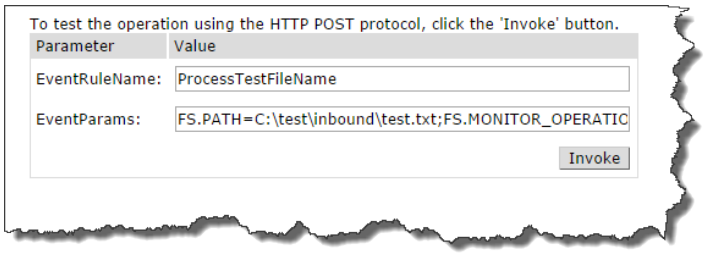


For this example, you can open the /**Backup/**folder and see that a backup file was created (for example, **C:\ProgramData\Globalscape\EFT Server\Backup**).

Using Web Service Examples

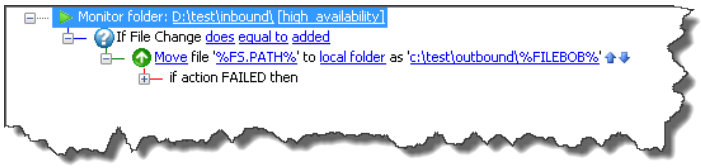
Folder Monitor






```
EventParams=FS.PATH=C:\test\inbound\test.txt;FS.MONITOR_
OPERATION=added
```

As you can see, the FS.MONITOR_OPERATION is part of the Condition and must be passed along with the variable of choice; in this case it is FS.PATH or any other variable that is created.




```
EventParams=FS.PATH=C:\test\inbound\test.txt;FS.MONITOR_
OPERATION=added;FILEBOB=test.filebob.txt
```

As you can see above, the variable is a custom variable applied to this event rule, outside of the EFT variables.

Timer Event

EventParams=FILEBOB=test.filebob.txt

The Timer Event is the least used Event Rule in EFT to download files, move them, or to automate an Advanced Workflow Script/custom command. Using the Web Services allows you to manipulate custom variables for the specific environment or file that needs to be processed. In the case above, the Timer event is being used as a transmission only, triggered by a remote process using “wget”.

Passing the URL to WebServices

As the HTTP GET states:

```
GET
/WebService/InvokeEventRule?EventRuleName=string&EventParams=str
ing
 HTTP/1.1
```

Based on this information, the URL should contain the following:

- **EventRuleName**=ProcessTestFileName
- **EventParams**=FS.PATH=C:\test\inbound\test.txt;
- **FS.MONITOR_OPERATION**=added

Combine the parameters:

```
http://localhost/WebService/InvokeEventRule?EventRuleName=Proces
sTestFileName&EventParams=FS.PATH=C:\test\inbound\test.txt;FS.MO
NITOR_OPERATION=added
```

> **NOTE:** The ampersand “&” is used to separate the **EventRuleName**and **EventParams**, but you will use the semi-colon (;) to separate more than 1 **EventParams**that is required to make the Event Rule work correctly.

Compression Action

(Requires EAM) Occasionally, users might upload or download files that need to be compressed (for example, zipped) or decompressed (for example, unzipped) before transferring. The Compress/Decompress Action can be used to compress and decompress files. You can compress/decompress the following formats: ZIP, 7Zip, GZip, BZip2, Tar, Tar and GZIP, and ZCompress. You can also enable/disable compression for files older than a defined time in days to meet PCI DSS compliance on retention and accessibility of logs.

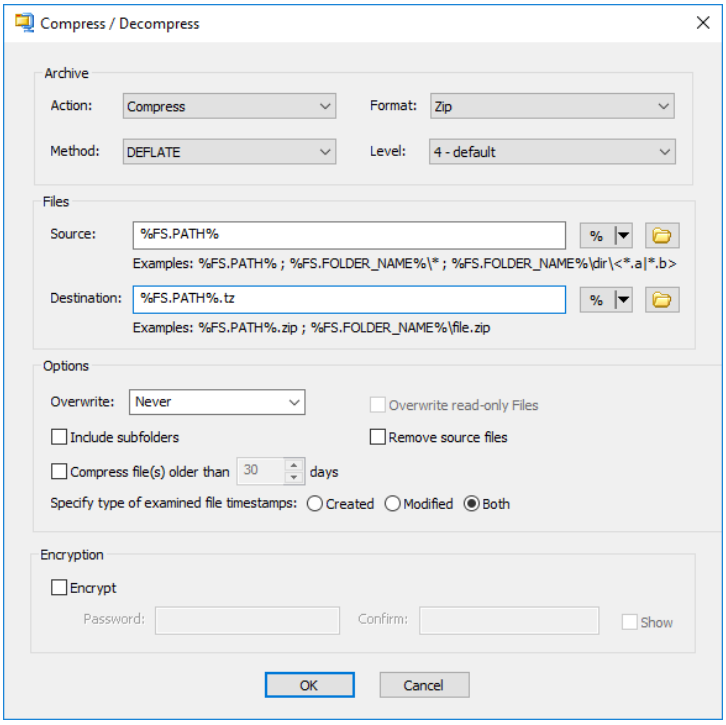
- To ensure maximum compatibility with third-party archival tools, Unicode passwords should be avoided.
- The **Source**and **Destination** file path specifications are limited to physical paths only – **virtual paths will not work for these fields**.
- For GZip format, add a trailing slash to the **Destination**path to make it explicitly clear that the destination is to be interpreted as a folder. If **Overwrite**is set to never, no error occurs, and the Action completes by removing the original GZip file.
- **Decompress Action Destination Paths and Trailing slashes (\):**

  If a user wants to decompress an entire archive and place it into a folder, using a destination path with a trailing slash (\) will always accomplish this. This is the typical use case and is shown in the example below the destination field. The only exception is if ZCompress is used, in which case the behavior is the same as for Zip, Tar, and 7zip as described below. If the trailing \ is missing, the behavior depends on the decompression format used:

  - For Zip, Tar, and 7zip archive formats it doesn't matter if the trailing \ is there, because the path will always be treated as the folder in which to decompress the entire archive. The exception to this is if the "< >" syntax is used where individual archive files and their destinations paths can be specified.
  - For Gzip, Bzip2, and "Tar and Gzip" (and ZCompress with or without trailing \) archive formats, only a single file whose name is the last part of the destination path will be extracted, decompressed, and saved into the parent folder specified in the destination path. So, if the destination path is given as "c:\myFolder\myFile", then a file named "myFile" will be extracted from the specified source archive, decompressed, and placed in "c:\myFolder" (with the same name).

To compress or decompress files using Event Rules

1. Add the Event to the Event Rule (for example, File Downloaded).
2. Add any (optional) Conditions.
3. Add the **Compression** Action.
4. Click any links in the action to open the **Compress/ Decompress** dialog box.



5. In the **Action**list, click the desired Action: **Compress**or **Decompress**.
6. In the **Format**box, specify the format in/from which to compress or decompress the file: ZIP, 7Zip, GZip, BZip2, Tar, Tar and GZIP, and ZCompress.
7. If the **Compress**Action is specified, in the **Method**list, specify the **Method**: Deflate or PPMd.
8. If the **Compress**Action is specified, in the **Level**list, specify a level of compression to apply, from **0 - fastest** to **6 - densest**.
9. If the **Decompress**Action is specified, the **Method**and **Level** lists are unavailable.
10. In the **Files**area, specify the **Source** and **Destination** paths. (As noted above, only physical paths should be specified; virtual path will not work.)
    - Select the variable drop-down list (percent sign **%**) to specify a context variable. You can specify more than one and use wildcards, as shown in the examples.

- Select the folder icon to browse to a folder. Add a trailing slash to the **Destination**path to make it explicitly clear that the destination is to be interpreted as a folder.

11. In the **Options**area, the **Overwrite** options (Never, **Always**, **If Newer**). **If Newer** is available when the Decompress Action is specified.
12. Select the check boxes to specify whether to **Include subfolders** (for Compress Action), **Overwrite read-only files**(for Decompress Action), and/or **Remove source files** after decompressing or compressing the file.
13. To compress files based on age, select the **Compress file(s) older than <n> days** check box and provide the number of days (default is 30 days), and next to **Specify type of examined file timestamps**, specify **Created**, **Modified**, or **Both** (the default is Both).

    > **NOTE:** The purpose of compressing older files is to move the compressed files to an archive folder (in a subsequent action or event rule) to meet PCI DSS 10.7 to retain audit trail history.

14. If encryption is desired, select the **Encrypt**check box and then specify and confirm the password. Select the **Show** check box to see if you've entered the password correctly.

Also refer to the following properties the ICICompressActionParams interface in the COM API

- Property **AllowOperationForOldFiles** As Boolean
- Property **KeepOldFilesInDays** As Long
- Property **TimestampTypeForOldFiles** as CompressTimestampType
- Enum **CompressTimestampType**

In the Backup and Cleanup event rule in EFT:

- Compress file action is added to the beginning of the event rule
- Compress files option is enabled with a default value of 90 days
- Type of examined file timestamps is set to “Both” by default
- “Cleanup in folder” is in EFT logs
- Number of days after which the file will be deleted in Cleanup action is only for the Logs folder. The default value is 275 days (previously 30 days)

Export to Dataset and Import CSV from Dataset Action

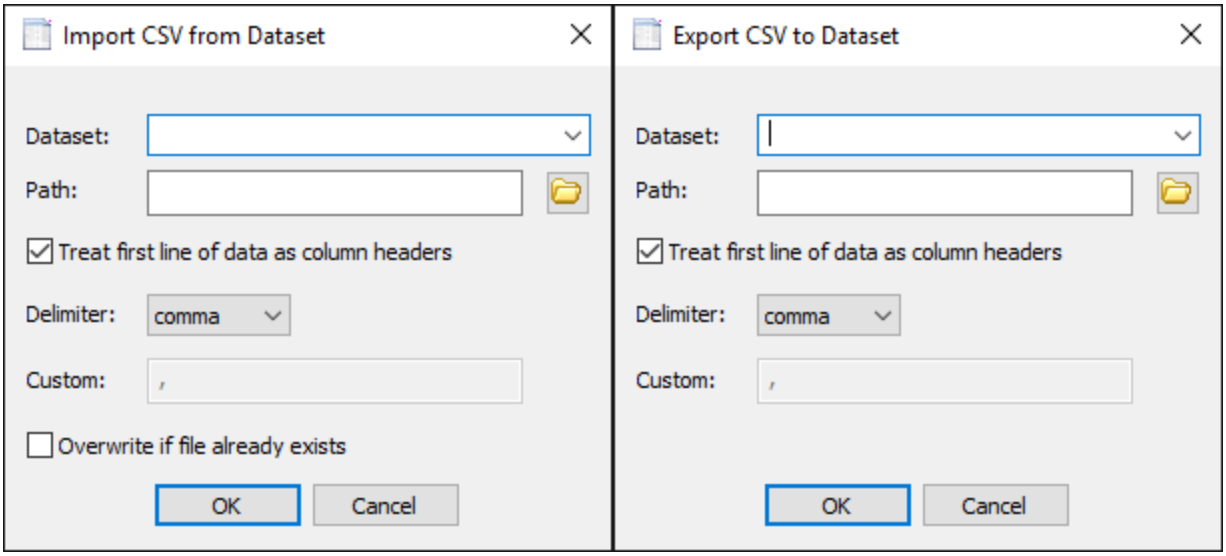
(Requires EAM) These CSV import/export actions can be used to move tabular data between programs that operate on incompatible, proprietary formats.

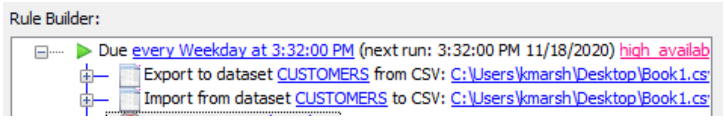
The **CSV: Import from Dataset** Action reads data from a comma-separated values (CSV) file, and populates the specified dataset with those values.

The **CSV: Export to Dataset** Action can be used in conjunction with Protocol: Listing to Dataset Action and Loop: Dataset(or with an existing dataset) to create a CSV file, which can then be used in other applications.

Refer to Datasets in Event Rulesfor information about using datasets in Event Rules.

In the **Dataset**drop-down in the **Export CSV**Action, do not specify a non-existent dataset, especially if you do not plan to dynamically create that dataset in the script via other means (such as PowerShell). If you specify a non-existent dataset, the action will fail and an error will appear in the EFT log (Export failed. Error: Dataset does not exist.)





CSV file format is not standardized; EFT allows multiple-character delimiter without any length limit. If the **Treat first line of data as column headers** check box is cleared, the dot notation for referencing the fields in records will be: Column0, Column1, Column2, and so on. For example, %Customer.CurrentRow.Column0%.

Related Topics

- Loop: Dataset Action
- Listing to Dataset Action
- Datasets in Event Rules

File Operation Action

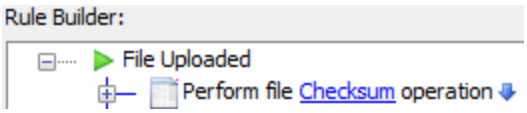
(Requires EAM) The File Operation Action is used to read, write, rename, delete, concatenate, or perform a checksum on files.

The COM API has been modified to address the changes to the File Operation Action. As a result, some COM objects are no longer supported as of version 8.0.5: ICIFileActionParams: Operation, Path, IncludeSubdirsFlag, Contents, Encoding, OverwriteOption, NewNameMask, ExclusionMasks, and UseExclusionMasksFlag.

Refer to the COM API referencefor details.

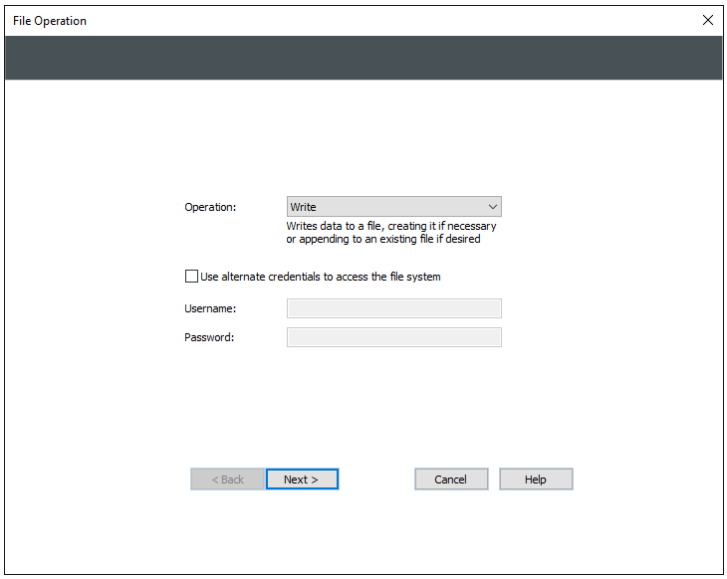
To define the File Operation Action

1. In the right pane, in the **Actions**list, add the **File: Operation**Action to the rule, then click the link in the rule to open the **File Action** dialog box. The Action appears in the Event in the **Rule Builder**.



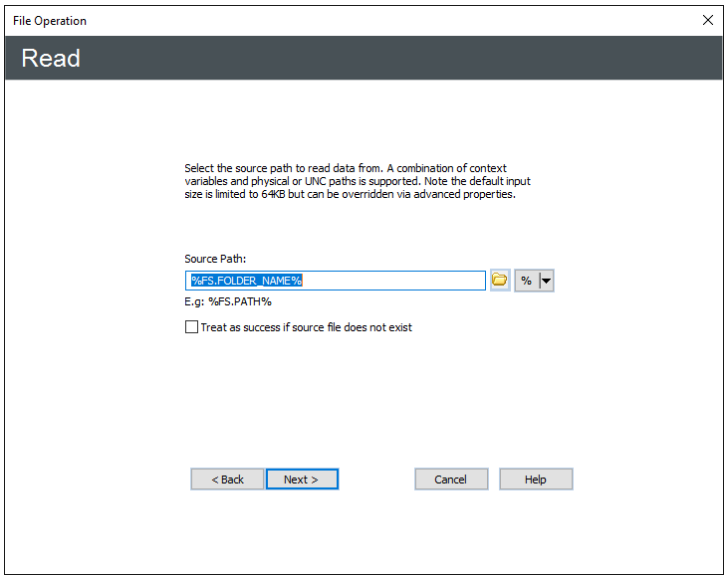
2. Select the linked text (blue or red) to specify parameters for the Action.
3. In the **Operation**list, click an operation:
   - **Read** - Read data from a file into a variable for processing (see note below)
   - **Write** - Write data to a file, creating the file if necessary, or appending to an existing file (see note below)
   - **Rename** - Rename and keep original (Copy) or remove the original (Move)
   - **Delete** - Delete one or more files
   - **Concatenate** - Concatenate the contents of two files and outputs the result into a destination file
   - **Checksum** - Obtain the hash for a file, which is useful for integrity checking

   By default, the File Action can only read or write 64KB of data. If you want to read and write more than 64KB, you will need to add the advanced properties MaxFileActionReadSize and MaxFileActionWriteSize and set the limits to how much you want to read/write. Refer to Advanced Properties for details.



4. (Optional) Select the **Use alternate credentials to access the file system** check box, then provide the **Username**and **Password** needed to log in. Otherwise, it will use the EFT server service account.
5. Click **Next**. The next page that appears depends on the operation selected, as shown below.
6. After defining the Action, click **Apply**to save the Action.

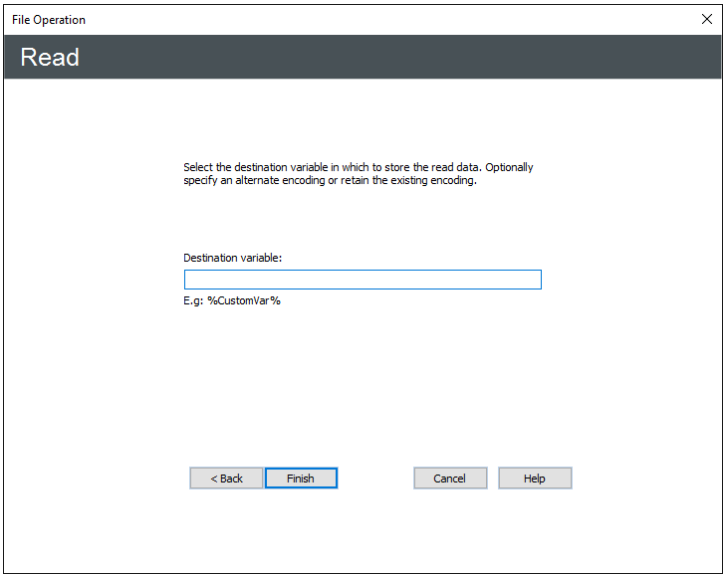
Read



a. Specify the **Source path** with variables or by selecting the folder icon and browsing.

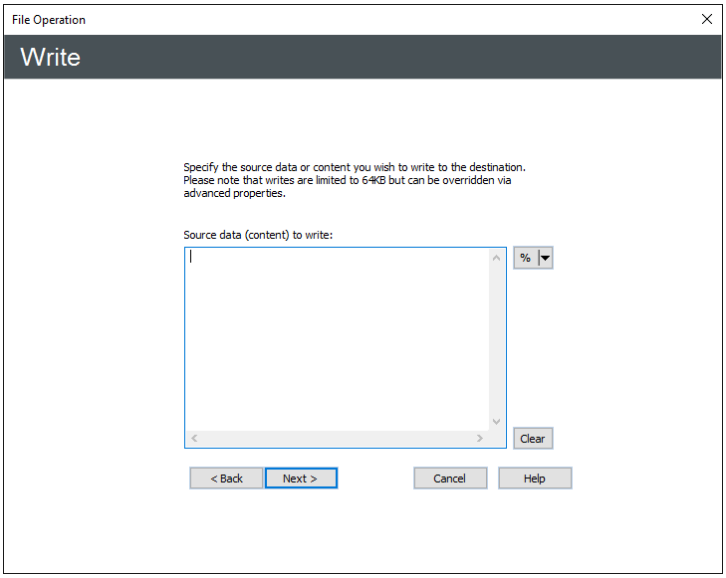
b. Select the **Treat as success if the source file does not exist** if you don't want this action to counted as a failure in that case.

c. Click **Next**.



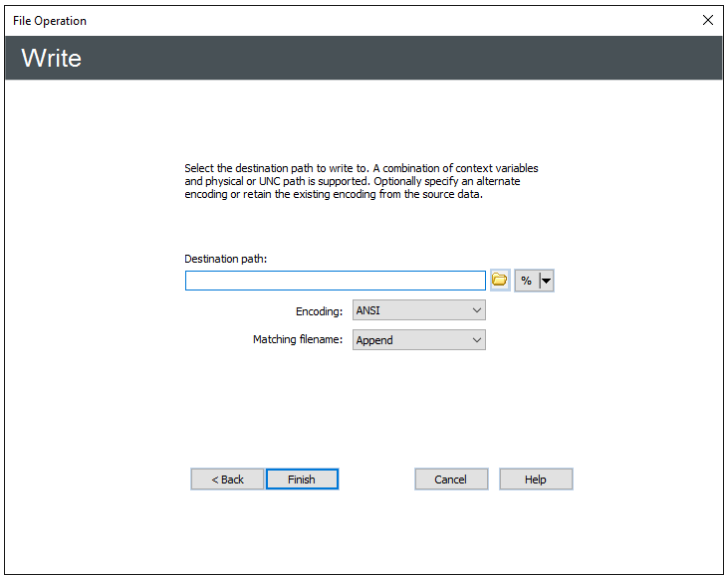
d. Specify the **Destination variable** into which to store the read data, then click **Finish**. Refer to Flow: Variable Action for details of creating variables.

Write



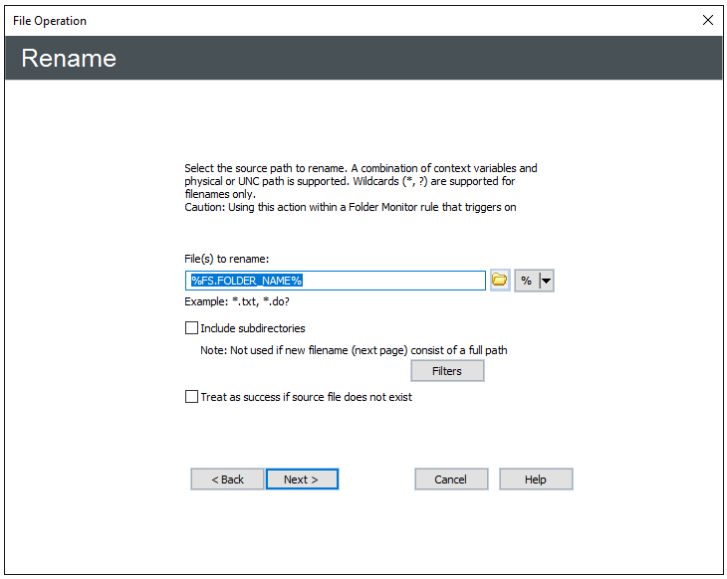
a. In the **Source data**box, specify the source data or content that you want to write to the destination. Writes are limited to 64KB, but that can be overridden via advanced properties.Use the variable (%) drop-down list to add EFT variables,

such as %FS.FILE_NAME%. Click **Next**.



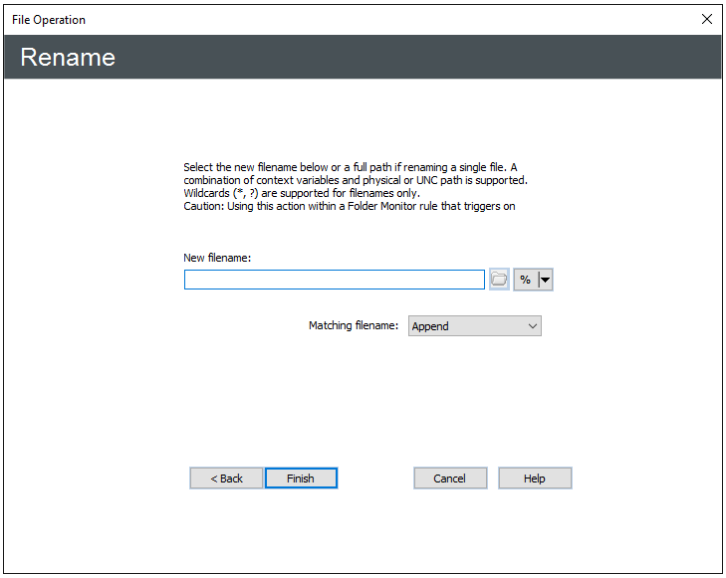
b. Specify the **Destination path** with variables or by selecting the folder icon and browsing.
c. Specify the **Encoding**(**ANSI**, **UTF8**, **Unicode**, **UnicodeBigEndian**), and what to do about a **Matching filename**(**Append**, **Skip**, **Numerate**, **Overwrite**, **Fail**), then click **Finish**.

Rename



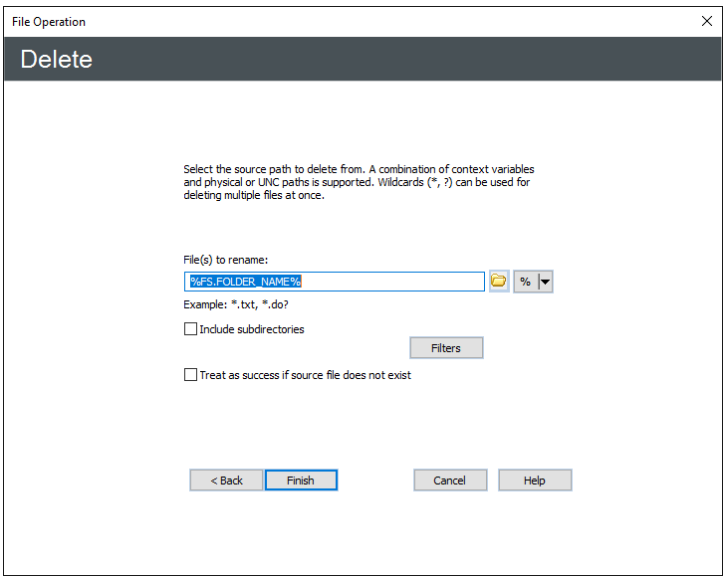
a. Specify the **File(s) to rename** with variables or by selecting the folder icon and browsing.

b. Select the **Include subdirectories** check box to rename subdirectories also. Do not select the check box if the new filename consists of a full path.
c. Select the **Treat as success if the source file does not exist** check box if you don't want this action to counted as a failure in that case.
d. Click **Next**.



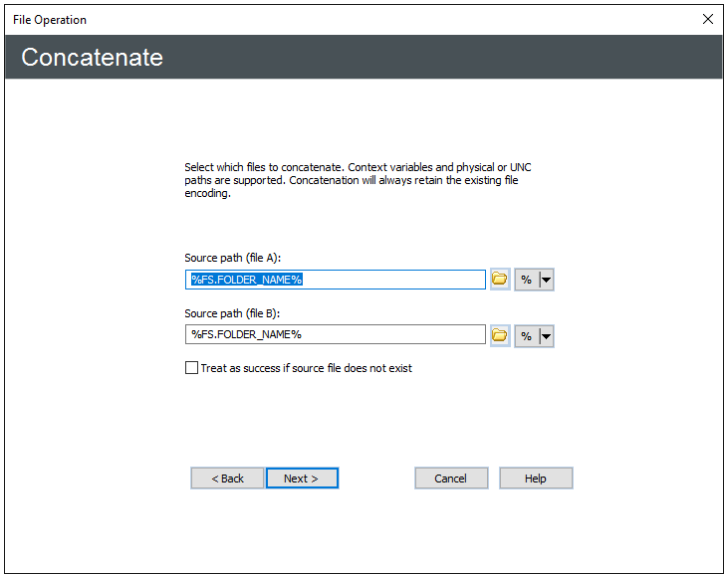
e. Specify the **New filename** with variables or by selecting the folder icon and browsing.
f. Specify what to do about a **Matching filename** (**Append**, **Skip**, **Numerate**, **Overwrite**, **Fail**), then click **Finish**.

Delete

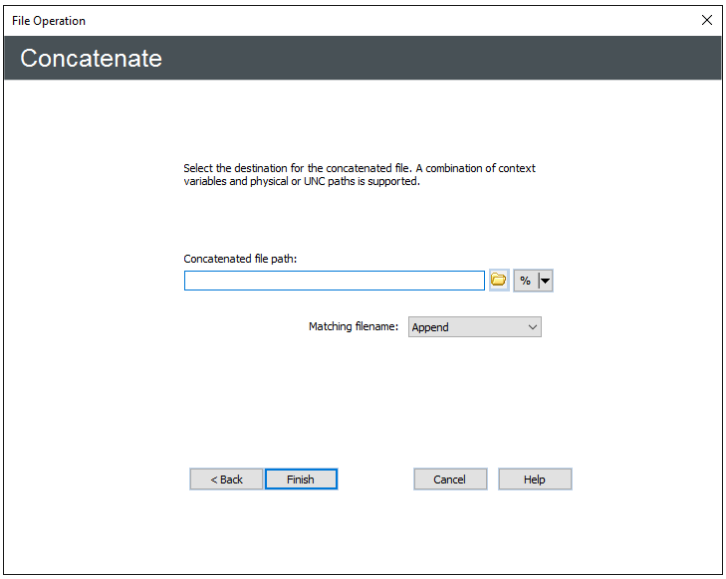


a. Specify the **File(s) to delete** with variables or by selecting the folder icon and browsing.
b. Select the **Include subdirectories** check box to rename subdirectories also. Click **Filters** to exclude one or more files. Specify multiple files and wildcards with commas. For example *.txt,*.pd?.
c. Select the **Treat as success if the source file does not exist** check box if you don't want this action to counted as a failure in that case.
d. Click **Finish**.

Concatenate

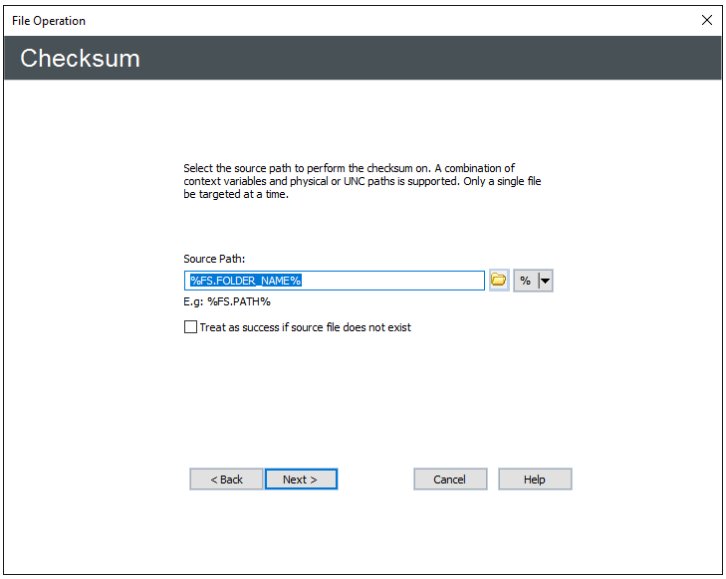


a. Specify the **Source path**for file A and file B with variables or by selecting the folder icon and browsing.
b. Select the **Treat as success if the source file does not exist** check box if you don't want this action to counted as a failure in that case.
c. Click **Next**.



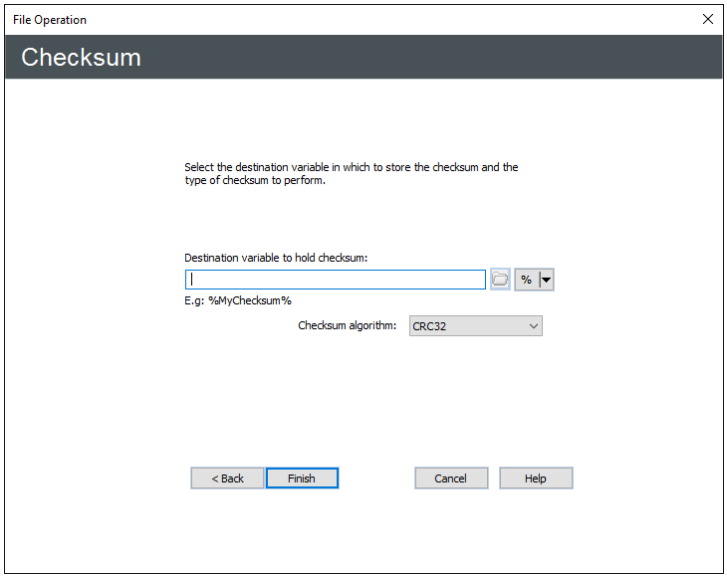
d. Specify the **Concatenated file path** with variables or by selecting the folder icon and browsing.
e. Specify what to do about a **Matching filename** (**Append**, **Skip**, **Numerate**, **Overwrite**, **Fail**), then click **Finish**.

Checksum



a. Specify the **Source path** with variables or by selecting the folder icon and browsing.

a. Select the **Treat as success if the source file does not exist** check box if you don't want this action to counted as a failure in that case.
b. Click **Next**.



a. Specify the **Destination path** with variables or by selecting the folder icon and browsing.
b. Specify the **Checksum algorithm** (**CRC32**, **MD5**, **SHA1**, **SHA256**, **SHA384**, **SHA512**) and then click **Finish**.

File: Scan Action

The **File: Scan** Action is used to send a file to an antivirus or data loss prevention scanner for processing.

- How does File: Scan work in Event Rules?
- File Scan Action Example
- File: Scan Action
- Scanning Metadata

Content Integrity Control

EFT's ICAP functionality is invoked through Event Rules, sending files to antivirus or data leak prevention (DLP) servers that detect file pass/fail based upon user-defined rules. Users can configure rules on a DLP server to send a reply to EFT with access denied if the file contains social security numbers (SSNs) or credit card numbers (CCNs), for example. Antivirus servers scan the files for viruses and return a response to EFT whether a virus was found or not. (Refer to File: Scan Action for the procedure for adding the action to an Event Rule.)

The Internet Content Adaptation Protocol (ICAP) is an HTTP-like protocol that is used for virus scanning and content filtering. According to RFC 3507:

ICAP is, in essence, a lightweight protocol for executing a "remote procedure call" on HTTP messages. It allows ICAP clients to pass HTTP messages to ICAP servers for some sort of transformation or other processing ("adaptation"). The server executes its transformation service on messages and sends back responses to the client, usually with modified messages. Typically, the adapted messages are either HTTP requests or HTTP responses.

On a DLP server, you can define rules to search files for SSNs or CCNs. For example, if you send a file containing a valid CCN, the DLP server will flag it and return a denied message to EFT. (To test this rule, you can put the universal test credit card number 4111 1111 1111 1111 in a text file and send it through the DLP via an EFT Event Rule.)

On an antivirus server, you can specify violation text in ICAP response headers: “X-Virus-ID:INFECTED” or ”X-Response-Info:blocked” or both (semicolon-separated).

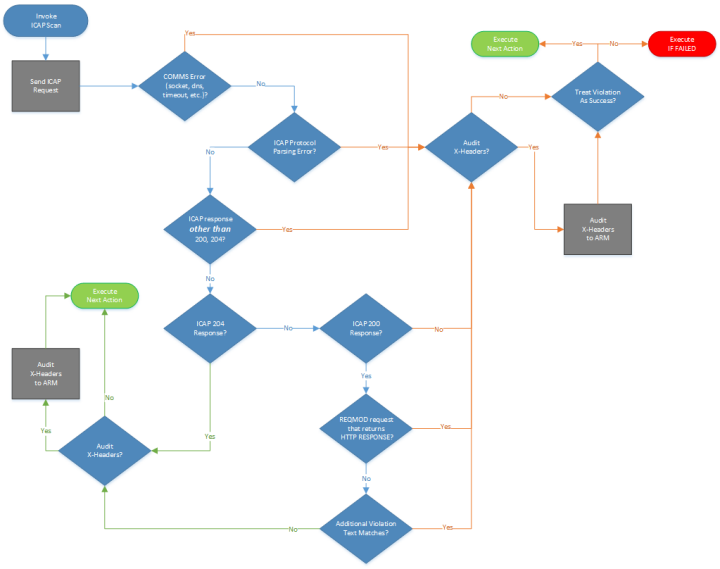
EFT does not return an error or any type of indicator from the Content Integrity Control Action if a file isn't completely processed/analyzed by an antivirus or DLP server due to the size of the file being larger than what is supported by that particular server. For example, MyDLP will process a maximum of 10 MB of data; if a flag is embedded in a file that is after the 10 MB limit, MyDLP will not detect the policy violation.

Suppose EFT sends an 11 MB file to myDLP, which has a max processing capacity of 10 MB. The myDLP server has a policy to return a failure for any files containing credit card numbers. The 11 MB file has a credit card number embedded at the end of file. As a result, the myDLP server would return to EFT that the Action was a success, because the myDLP server did not process the credit card number.

Refer to Content Integrity Control Tab for details of creating a CIC profile.

Content Integrity Control Actions are also captured in the EFT log, after you enable `#log4cplus.logger.Events.ContentIntegrityControl=TRACE`in the logging.cfgfile. (Remove the # in front of that line.)

Below is a diagram demonstrating EFT decision points for Content Integrity Control (ICAP) success or failure.



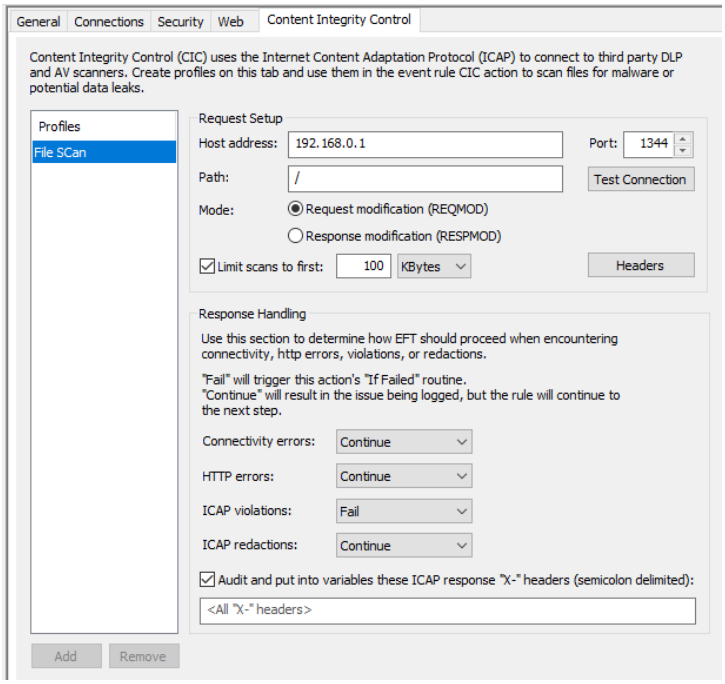
Related Topics

- Content Integrity Control Tab
- File: Scan Action
- EFT Specifications
- logging.cfg

Content Integrity Control Tab

Content Integrity Control is used to send a file to an antivirus scanner or data loss prevention solution for processing. When a **File Scan** Action is added, a file that triggers the Event Rule is sent to an ICAP server for processing. When the file passes, other Actions can occur, such as moving the file to another location. If the file fails, processing can stop, or other Actions can occur, such as sending an email notification.

Refer to Global Antivirus Scanning for details of configuring Global antivirus on this tab.



To remove a profile

- To remove a profile, select its name in the list, and then click **Remove**.

Related Topics

- Global Antivirus Scanning
- File: Scan Action (CIC)
- EFT Specifications

How does File: Scan Work in Event Rules?

The **File: Scan** Action is used to send a file to an antivirus or data loss prevention scanner for processing. When this Action is added, a file that triggers the Event Rule is sent to an ICAP server for scanning. When the file passes the scan, other Actions can occur, such as moving the file to another location. If the file fails the scan, processing can stop, or other Actions can occur, such as sending an email notification. EFT fully supports RFC3507 section-3.1 and section-4.8. EFT can adapt the outgoing response if the ICAP server indicates that adaptation is necessary.

How does File: Scan work in Event Rules?

The **File: Scan** Action allows ICAP clients to pass HTTP messages to ICAP servers to scan the file(s) in the Event Rule that is passing through EFT.

You can create reusable profiles on the Content Integrity Control Tab and you can create a custom Content Integrity Control (CIC) profile as you need it, as described below.

Important info about how EFT uses the File Scan Action

IMPORTANT:

- Using the File Scan Action with encrypted files will not return an accurate result. Copy/move the files to a folder that is not encrypted to process with the ICAP server.
- ICAP servers don't all offer the same features. The action was tested with:
  - Clearswift version 5
  - Symantec DLP version 14.5.0.24028
  - Kaspersky version 5.5
- When using the action, EFT needs to use POST in HTTP requests. Refer to knowledgebase article https://kb.globalscape.com/KnowledgebaseArticle11375.aspxfor information about enabling an advanced property.
- **File Uploaded** and **Workspace Created** events are triggered after a file is uploaded and after a Workspace is created. Only after the event triggers will the action begin communication with the ICAP server, and then redacts the file, if needed. Therefore, there may be delays between when a Workspace is created and a file is redacted. Use the **File Uploaded** event to trigger the action, then use the **File: Scan** action and "Fail" to prevent the message from being sent. Use the **Before Download**event trigger to scan the file before it's downloaded.

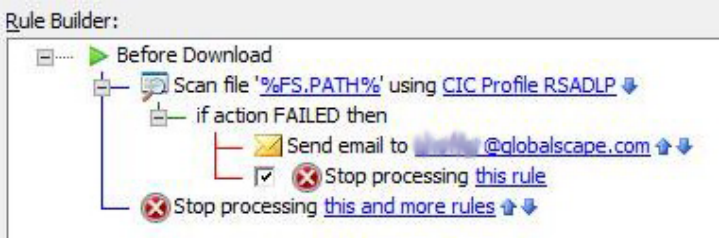
.

Scan a File Using the File: Scan Action

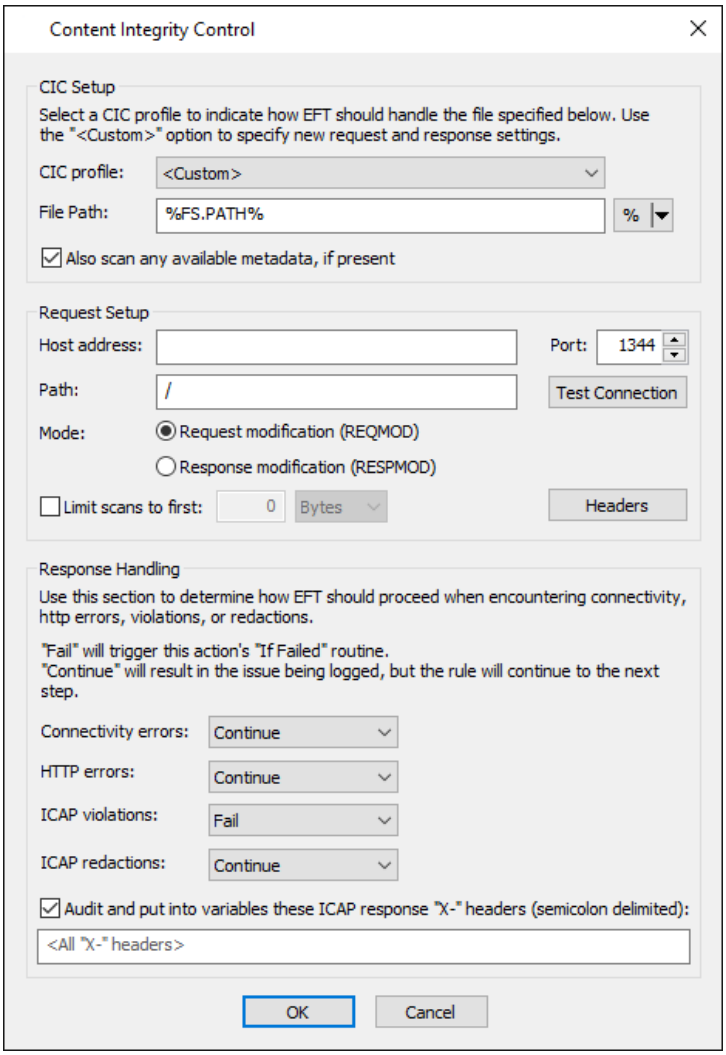
The **File: Scan** Action is used to send a file to an antivirus or data loss prevention scanner for processing.

To scan a file using the File: Scan Action

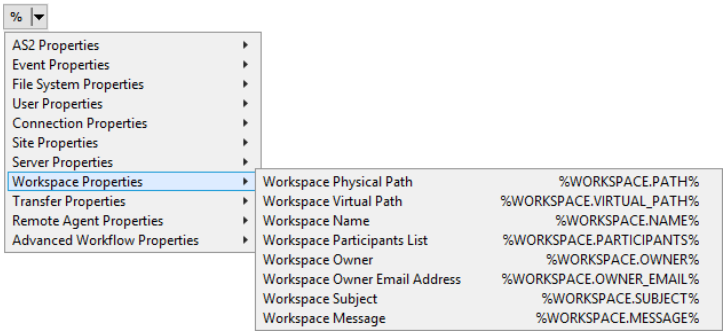
1. Create a new Event Rule, such as a Folder Monitor Event.
2. Add relevant Conditions.
3. Add the **Content Integrity Control** Action. For example:



4. In the Action, click either of the underlined/linked items. The **Content Integrity Control**dialog box appears.

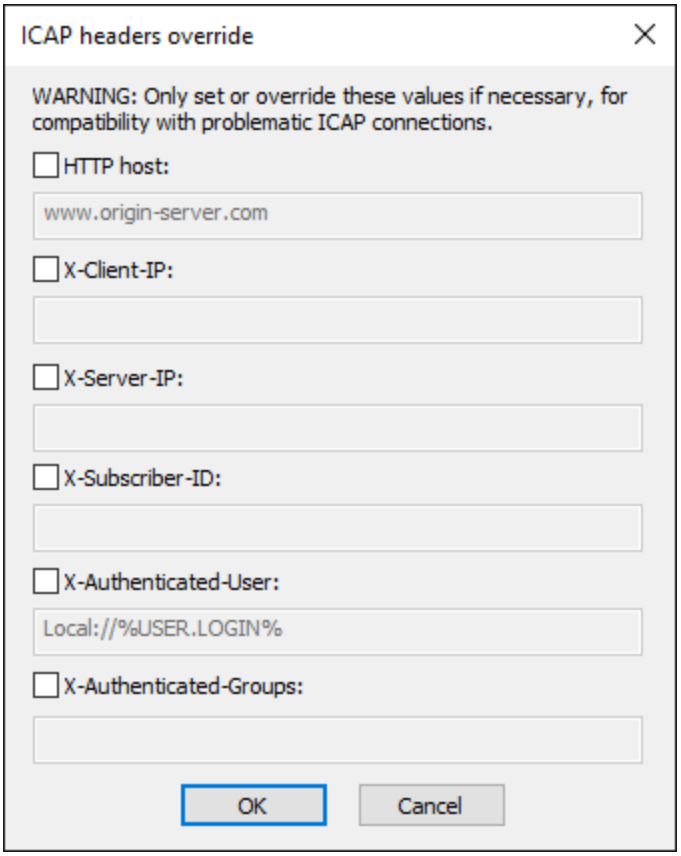


5. Click the **CIC Profile**drop-down list to select a predefined profile, or select **<Custom>**.
6. **File Path**- Physical location of the file to send to the ICAP server; %FS.PATH% is the default. You can specify another variable or drive and UNC paths. Wildcards are unsupported.
    - **%** - Click the drop-down list if you want to specify other context variables:



7. **Also scan any available metadata, if present** - Metadata includes the field name of Workspaces send operations. Consult your ICAP server for detailed information. The check box is selected by default.
    - The context variables Workspace Subject (%WORKSPACE.SUBJECT%) and Workspace Message (%WORKSPACE.MESSAGE%) (see above) relate to this feature.
8. If you specified a <Custom> profile, complete the rest of the fields in the dialog box:
    a. **Host address**, **Path, Port** - These settings depend on settings in the antivirus or DLP (ICAP) server.
        - The **Host address** field should be the URL of the ICAP server (the field cannot be blank).
        - By default, the port is set to 1344.
    b. **Test Connection** - After you specify the connection to the ICAP server, test the connection. If connection fails, verify these settings match the settings defined in the antivirus or DLP solution. (In earlier versions, **Test Connection** doesn't work with %variable% in the connection field.)
    c. **Mode** - Specify one of the following:
        - **Request modification (REQMOD)** - - Request modification mode: Embeds file contents in an HTTP PUT request body, which is then sent in the body of an ICAP request to the server. The ICAP server may respond with a modified version of the embedded request, or a new HTTP response. The ICAP response will depend on your ICAP server's implementation.
        - **Response modification (RESPMOD)** - Response modification mode: Embeds file contents in an HTTP 200 OK response body, which is then sent in the body of an ICAP request to the server. The ICAP server may respond with a modified version of the embedded response. The ICAP response will depend on your ICAP server's implementation.
    d. **Limit scans to first *n*bytes** - (Optional) Specify the number of bytes to scan. Some antivirus solutions only require a subset of a file's contents to test against their database of malware signatures. To keep from transferring large files in their entirety when we only need the first *n* bytes, you can specify how many bytes are sent to the ICAP server. When this check box is cleared, the entire file is transferred to the ICAP server. If the file is smaller than the Max scan size, the entire file will be transferred for scanning.

9. **Headers** - (Optional) In v8.0.5 and later, only set these values if needed for problematic ICAP connections. Headers can be used to override the REQMOD/RESPMOD X-headers sent by EFT, to fine-tune the connection to the ICAP server. These headers are displayed in the ICAP server logs.



- **HTTP host** - The EFT site's local host address (do not use "localhost"); The default is to show the EFT HTTP Host if supplied (not localhost), otherwise "www.origin-server.com"; If you override the Host value, then that value is used instead. The order is: user override value -> EFT HTTP Host if supplied (not localhost) -> or www.origin-server.com as last resort.
- **X-Client-IP** - Blank by default
- **X-Server-IP** - Blank by default
- **X-Subscriber-ID** - Blank by default
- **X-Authentication User** - Provide a string with variables.
  - **LDAP** - Example: "LDAP://pdc/samaccountName=%LOGIN.LOGIN%,DC=s5development,DC=local"
  - **AD** - Examples: WinNT://{NetBIOSDomainName/sAMAccountName}, WinNT://pdc/s5dev\arybin

- **Other**- Examples: Local://%USER.LOGIN%, Local://%SERVER.NODE_NAME%
- **X-Authenticated Groups** - Blank by default
- User can override and use context variables if desired as field elements. EFT will base-64 encode.

Note the difference between "ICAP Header" and "HTTP Header." The ICAP Header is a header with service information EFT sends to the ICAP server. The HTTP header is a part of information EFT sends to ICAP for analysis. That is, the HTTP header will be analyzed, not the ICAP header. The HTTP header is shown in ICAP log files.

10. Under **Response Handling**:
    - Specify whether transfer should **Continue**or **Fail** when the following occur: **Connection errors**, **HTTP errors**, **ICAP redactions**.
11. **Audit and put into variables these ICAP response "X-" headers** - (Optional) Specify “X-“ headers for auditing using ARM. If this option is enabled and no “X-“ headers are specified, all “X-“ headers will be audited. Use semicolons between multiple items. Note this check box only affects whether the specified headers are audited by ARM, regardless of success or failure.
12. Click **OK** to save the changes in the Event Rule. The name of the profile appears in the Event Rule Action.

Related Topics

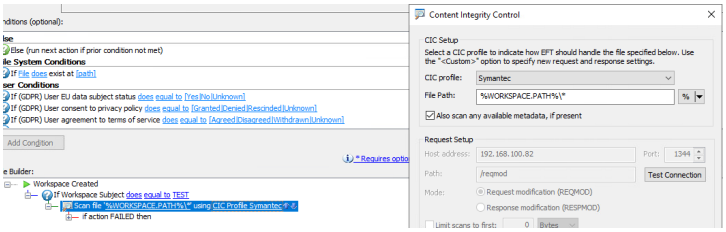
- Content Integrity Control
- Content Integrity Control Tab

Scanning Metadata

In general, "metadata" is "data that provides information about other data." Metadata does not provide the content of the data, such as the text of a message or an image itself. In Workpaces, for example, metadata can be subject, message, and attached file of a Workspaces message. The File: Scan action scans metadata to look for ICAP violations in the content, such as a full credit card number.

To test the metadata feature

1. Create an Event Rule using the **Workspace Created** event.
2. Add the **If Workspace Subject**Condition with the subject **does equal to** TEST.
3. Add the **File: Scan** Action.
4. Specify your ICAP server or use your CIC profile to scan the files.
5. In the **File Path** box, select the variable **%WORKSPACE.PATH%**, then add a backslash and an asterisk: *****. This will ensure the attached file is scanned.
6. Select the **Also scan any available metadata, if present** check box. This will ensure the metadata are scanned.



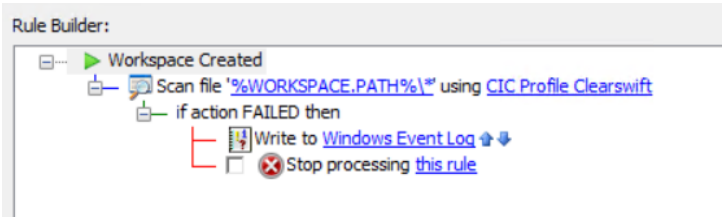
7. Save and run the Event Rule. The subject, message, and attached file will be scanned when using the Web Transfer Client to send a file. The message will be flagged if there are any violations in the message due to ICAP policy.

   Since you cannot predict what information will be in the Subject or Message, you can add an "if action FAILED" action, such as an email notification or Write to Windows Event Log, instead of a Condition.

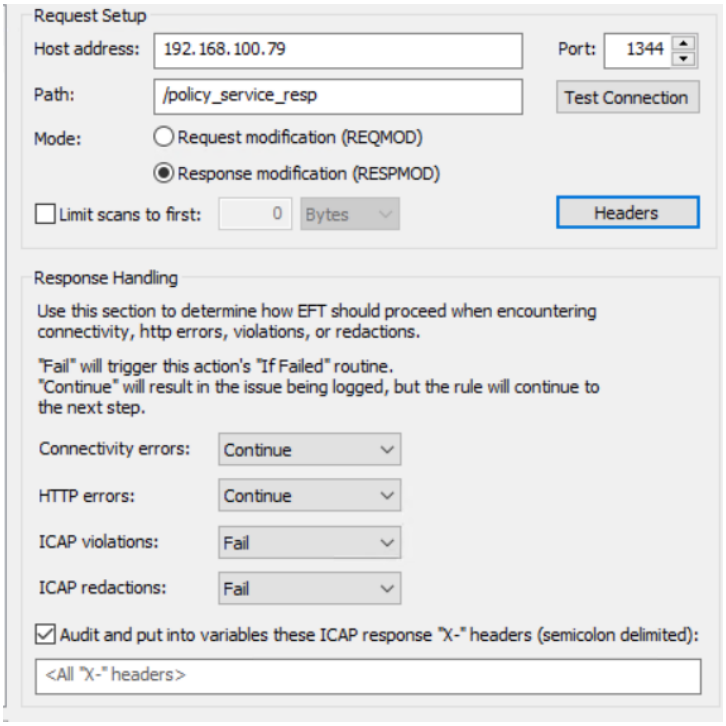
File Scan Action Example

Below is an example of a **Workspace Created** Event Rule with a **File Scan** Action and an **if action failed**action to **Write to Event Log.**

In this example, when a Workspace is created, the File Scan action uses the Clearswift profile to scan any files in that Workspace when it was created. If the scan finds any ICAP violation or redactions, it writes the information to the Windows Event Log. A file in the Workspace named BadCreditCard.txt contains a credit card number, which will fail the File Scan.

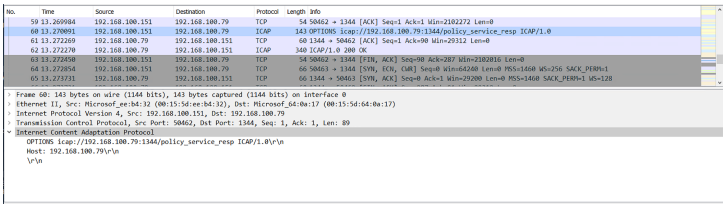


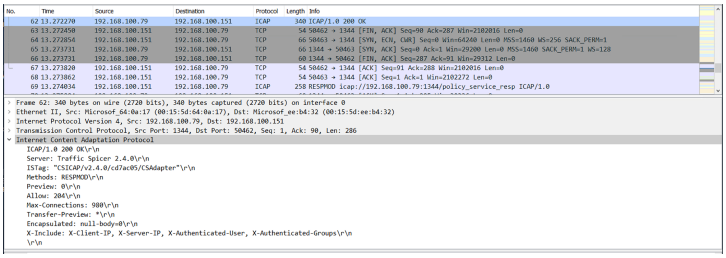
The profile was configured to work with a Clearswift ICAP server.



Details of the RESPMOD messages using Wireshark:

An example of EFT sending the Option method to a Clearswift ICAP server and the ICAP response:





Subject of a message sent with a file:

```
RESPMOD icap://192.168.100.79:1344/policy_service_resp ICAP/1.0
Host: 192.168.100.79
Allow: 204
X-Authenticated-User: TG9jYWw6Ly9keWVsYWNpYw==
Encapsulated: req-hdr=0, res-hdr=58, res-body=162

GET /BadCreditCard.txt HTTP/1.1
Host: 192.168.100.151

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 14
Cache-Control: no-cache

e
Subject Matter
0

ICAP/1.0 204 No Content
Server: Traffic Spicer 2.4.0
ISTag: "CSICAP/v2.4.0/cd7ac05/CSAdapter"
```

Message sent with the file:

In the Wireshark readout, you can see the contents of the message:

```
411 1111 1111 1111
  Now is the time...
```

and then at the bottom of the file, you can see the credit card number was redacted:

```
**** **** **** ****
Now is the time
...
RESPMOD icap://192.168.100.79:1344/policy_service_resp ICAP/1.0
        Host: 192.168.100.79
        Allow: 204
        X-Authenticated-User: TG9jYWw6Ly9keWVsYWNpYw==
        Encapsulated: req-hdr=0, res-hdr=58, res-body=162

        GET /BadCreditCard.txt HTTP/1.1
        Host: 192.168.100.151

        HTTP/1.1 200 OK
        Content-Type: application/octet-stream
        Content-Length: 39
        Cache-Control: no-cache

        27
        4111 1111 1111 1111
        Now is the time ...
        0

        ICAP/1.0 200 OK
        Server: Traffic Spicer 2.4.0
        ISTag: "CSICAP/v2.4.0/cd7ac05/CSAdapter"
        X-Virus-ID: Credit Card Numbers
        X-Infection-Found: Type=1; Resolution=1; Threat=Credit
Card Numbers;
        X-Violations-Found: 1
        BadCreditCard.txt
        Credit Card Numbers
        0
        1
        Encapsulated: res-hdr=0, res-body=104

        HTTP/1.1 200 OK
        Content-Type: application/octet-stream
        Content-Length: 39
        Cache-Control: no-cache

        27
        **** **** **** ****
        Now is the time ...
        0
```

```
  File contents scanned and redacted:
        RESPMOD icap://192.168.100.79:1344/policy_service_resp
ICAP/1.0
        Host: 192.168.100.79
        Allow: 204
        X-Authenticated-User: TG9jYWw6Ly9keWVsYWNpYw==
        Encapsulated: req-hdr=0, res-hdr=58, res-body=163

        GET /BadCreditCard.txt HTTP/1.1
        Host: 192.168.100.151

        HTTP/1.1 200 OK
        Content-Type: application/octet-stream
        Content-Length: 341
        Cache-Control: no-cache

        155
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        fubar
        0

        ICAP/1.0 200 OK
        Server: Traffic Spicer 2.4.0
        ISTag: "CSICAP/v2.4.0/cd7ac05/CSAdapter"
        X-Virus-ID: Credit Card Numbers
        X-Infection-Found: Type=1; Resolution=1; Threat=Credit
Card Numbers;
        X-Violations-Found: 1
        BadCreditCard.txt
        Credit Card Numbers
        0
        1
        Encapsulated: res-hdr=0, res-body=105
```

```
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 341
Cache-Control: no-cache

155
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
**** **** **** ****
fubar
0
```

EFT Log has the following information for this example:

```
02-05-21 13:18:23,255 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Processing
 Content Integrity Control request for profile [2576e336-6a20-
4d35-af8d-81094e4fa91c],
 file
[C:\InetPub\EFTRoot\MySite\Usr\<username>\WorkspacesSendMessage
\Subject
 Matter\\*], scan metadata: 1
       02-05-21 13:18:23,255 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Checking
 file:
C:\InetPub\EFTRoot\MySite\Usr\<username>\WorkspacesSendMessage\
Subject
 Matter\\BadCreditCard.txt
       02-05-21 13:18:23,271 [1216] ERROR
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
```

```
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - ICAP
redaction
 found during CIC action, file
[C:\InetPub\EFTRoot\MySite\Usr\<username>\WorkspacesSendMessage\
Subject
 Matter\\BadCreditCard.txt], profile[Clearswift] action failed.
        02-05-21 13:18:23,271 [1216] WARN
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Content
 of file:
'C:\InetPub\EFTRoot\MySite\Usr\<username>\WorkspacesSendMessage\
Subject
 Matter\\BadCreditCard.txt' was redacted.
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Infection-Found: Type=1; Resolution=1; Threat=Credit Card
Numbers;]
 in response.
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Infection-Found%: " Type=1;
Resolution=1;
 Threat=Credit Card Numbers;"
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Violations-Found: 1] in response.
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Violations-Found%: " 1"
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Virus-ID: Credit Card Numbers] in response.
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Virus-ID%: " Credit Card
```

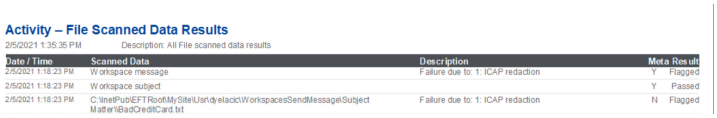
```
Numbers"
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Auditing
 these X headers [X-Infection-Found: Type=1; Resolution=1;
Threat=Credit
 Card Numbers;;X-Violations-Found: 1;X-Virus-ID: Credit Card
Numbers]
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Scanning
 workspace subject
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Checking
 metadata: Workspace subject
        02-05-21 13:18:23,287 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Scanning
 workspace message
        02-05-21 13:18:23,287 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Checking
 metadata: Workspace message
        02-05-21 13:18:23,302 [1216] ERROR
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - ICAP
redaction
 found during CIC action, metadata[Workspace message], profile
[Clearswift]
 action failed.
        02-05-21 13:18:23,302 [1216] WARN
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Overriding
 existing event context property %WORKSPACE.MESSAGE%
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Define
 event context variable %WORKSPACE.MESSAGE%: "**** **** ****
****
        Now is the time ..."
```

```
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Infection-Found: Type=1; Resolution=1; Threat=Credit Card
Numbers;]
 in response.
        02-05-21 13:18:23,302 [1216] WARN
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Overriding existing event context property %X-Infection-Found%
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Infection-Found%: " Type=1;
Resolution=1;
 Threat=Credit Card Numbers;"
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Violations-Found: 1] in response.
        02-05-21 13:18:23,302 [1216] WARN
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Overriding existing event context property %X-Violations-Found%
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Violations-Found%: " 1"
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Virus-ID: Credit Card Numbers] in response.
        02-05-21 13:18:23,302 [1216] WARN
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Overriding existing event context property %X-Virus-ID%
        02-05-21 13:18:23,318 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
```

```
 Define event context variable %X-Virus-ID%: " Credit Card
Numbers"
        02-05-21 13:18:23,318 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Auditing
 these X headers [X-Infection-Found: Type=1; Resolution=1;
Threat=Credit
 Card Numbers;;X-Violations-Found: 1;X-Virus-ID: Credit Card
Numbers]
        02-05-21 13:18:23,318 [4124] INFO SMTP <> - The
 number of messages are pending for send: 1
```

The ARM Report:

The report displays the failure of the message, and that the file was redacted.



Activity – File Scanned Data Results

2/5/2021 1:35:35 PM Description: All File scanned data results

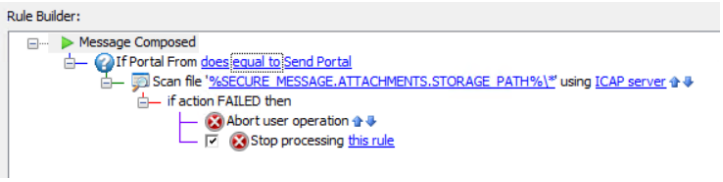
Date / Time	Scanned Data	Description	Meta	Result
2/5/2021 1:18:23 PM	Workspace message	Failure due to: 1: ICAP redaction	Y	Flagged
2/5/2021 1:18:23 PM	Workspace subject		Y	Passed
2/5/2021 1:18:23 PM	C:\InetPub\EFTRoot\MySite\Users\dyelack\WorkspacesSendMessage\Subject Matter\IBadCreditCard.txt	Failure due to: 1: ICAP redaction	N	Flagged

Flow: Abort User Operation

The **Flow: Abort User Operation** action is used to allow administrators to abort a user's requested operation. The action is only available with the **Message composed** event trigger.

For example, using the Event Rule as defined below, when a user defines a message in the Send portal and attempts to send a file that contains a credit card number, the file is sent to the ICAP server to be scanned and then the file is blocked or redacted because of the credit card number and moved to a quarantine location.

In this case, the **Abort user operation** action blocks the message from being sent, the user receives a failure message, and the Workspace is not created.



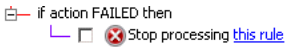
- This action cannot be configured to run asynchronously.
- The ICAP server
- The response code is always 403; the Advanced Property, AbortUserOperationHTTPCode can be used to set a different value.
- The response message is derived from EFT message templates for HTTP response codes.
- The headers sent back are the standard ones used for a normal failure situation.

Flow: Stop Processing Action

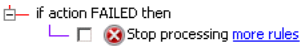
The *Stop Processing* Action is added automatically with each of the Actions except for the Send notification email Action, or you can add it after an Event or Condition.

When importing event rules from version 8.0 or later, the multi-line "Create or set variable" event action will import with the multiple lines. When upgrading, this path removes the multiple lines. The event rule will end up with a single "create or set variable" event rule action.

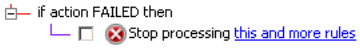
The Stop Processing Action ends processing of Event Rules, depending on your selection:



- **this rule**—The current Rule is aborted, and the next Rule in order is started. That is, it only affects subsequent Actions for THIS Rule. Other matching Rules will continue to process.



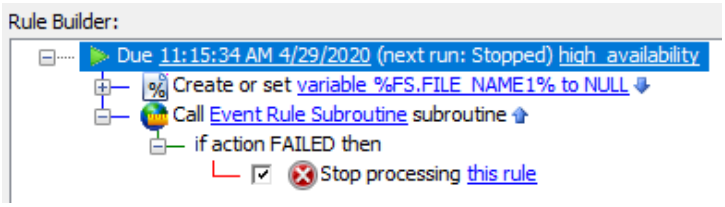
- **more rules**—The current Rule continues executing, the next Rules in order are not started. That is, it allows the current Rule to complete its processing, but no further matching Rules will continue to process.



- **this and more rules**—The current Rule is aborted, and the next Rules in order are not started. That is, stop any subsequent Actions for this Rule and don't process any subsequent matching Rules.

Action lines are collapsed by default, if no "if failed" values are set.

- The line is collapsed by default if no if-failed action is specified
- The line is expanded by default if an if-failed action is specified

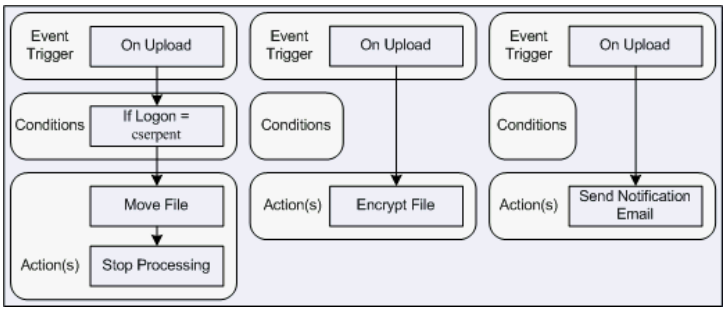


- The Create or set variable action does not have an "if action failed" option

Some exceptions/clarifications to consider:

- Folder Monitor and Timer Rules are not ordered, because there is only one Rule corresponding to a specific Folder Monitor/Timer (“one Event - one Rule” correspondence); only “Stop processing this Rule” is available for them. Certain “server-wide” Events (“Monitor Folder Failed,” “Service started,” “Service stopped,” “Log rotated”) allow “Stop processing this Rule” behavior only.
- The Stop Action affects only the current Event; when a client uploads the next file (that is, when the next “File Uploaded” Event happens), EFT will execute all Rules (from first to last) again.

The example below shows three Rules that are triggered with an On Upload Event. "Stop processing this and more Rules" causes the other two processes in this example to stop:



Based on these Rules, cserpent's file will be moved, but uploaded files will not be encrypted, nor will cserpent receive an email notification when a file is uploaded.

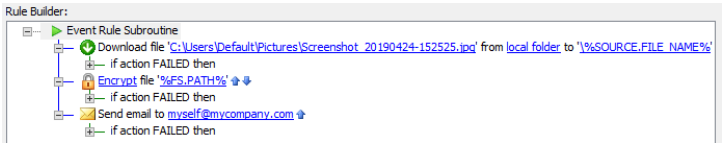
A recurring Timer does not stop recurring if the Rule Actions fail; it will recur as scheduled until you disable or delete the Rule. In the case of Timer Rules, "Stop processing this rule" means "do not execute any further Actions with this Rule" (such as sending an email), but it does NOT mean that the Timer will stop. For example, if you have defined the Rule to run every hour, an Action in the Rule could fail (such as downloading a file from a remote computer), but the Timer will run again the next hour, and the next hour, and so on, until you tell it to stop (by manually disabling it).

Flow: Subroutine Action

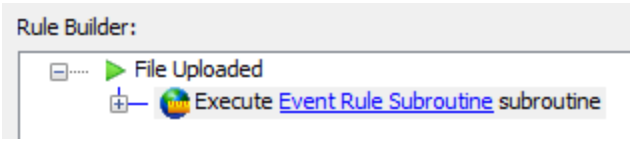
(Requires EAM) The **Flow: Subroutine** Action allows you to call an Event Rule Subroutine event trigger from within another event rule. The primary purpose of the Flow: Subroutine action is to help you break up larger rules into smaller, reusable ones. Obviously, you would have already created other rules to call. These sub tasks would be rules that you commonly use, such as sending email notifications, moving files, encrypt/decrypt, and so on.

To create an event with the Subroutine action

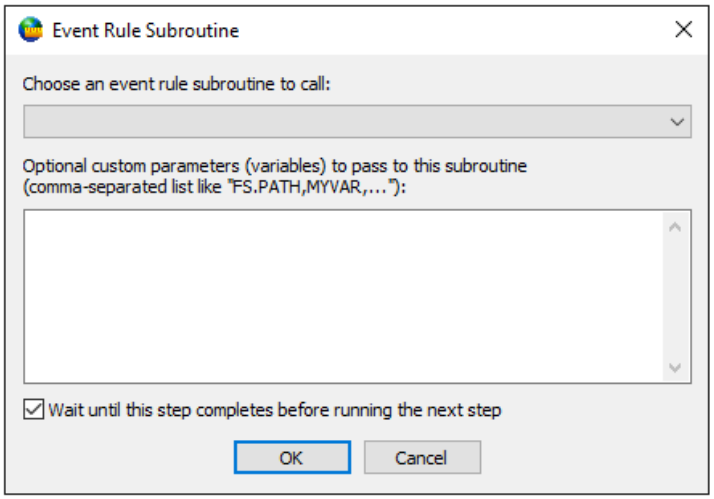
1. First use the Event Rule Subroutine event trigger to create a subroutine that contains frequently used actions.



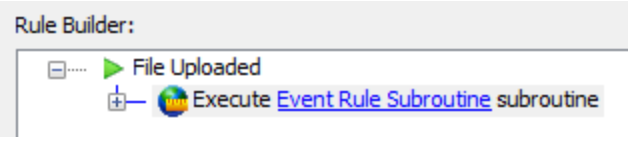
2. Then Create a new event ruleand add the **Flow: Subroutine**action to the Event Rule.



3. Click the link in the action to open the **Event Rule Subroutine** dialog box.



4. Click the **Choose a rule to trigger** drop-down list to specify which event rule to trigger, and then specify parameters (variables) to pass to the rule (optional).
5. (Optional) The **Wait until this step completes before running the next step** check box is selected by default. When the check box is selected, you can select the "If failed" action, and populate it with actions to run in case the rule fails. To allow the next step to run before this action completes, clear the check box. If check box is not selected, a prompt appears to confirm: "This step will be executed asynchronously (non-blocking), which means EFT won't wait for this step to be completed before running the next step. This could yield undesirable results if the next step depends on the output or outcome of this one. Are you sure you want to make this action asynchronous?" (All actions in the IF FAILED section are lost if the parent action is switched from async to sync mode.)



6. Click **OK** to close the **Event Rule** dialog box and accept the changes.

Notes:

- If there is no FAILED action set, then the call to the subroutine is asynchronous, and the subroutine is placed into a queue.
- The number of threads serving the queue, which applies to all Sites on a server, (that is, executing async subroutines) is defined by the **RunningAsyncSubroutinesLimit**advanced property. The default is 10; 0 equals no limit
- The per-Site limit on queue size is defined by the **QueuedAsyncSubroutinesLimit**advanced property. The default is 0, which equals no limit.
- The Events logger should be used for troubleshooting.

Related COM API objects:

- **EventRuleSubroutine**value is added to **EventType**enum
- **RunEventRuleAction** value is added to **EventActionType**enum
- **ICIRunEventRuleActionParams**interface is added to allow new action handling with two read/write properties:
  - [string] RuleName - the name of the subroutine to invoke [array of strings]
  - Variables - the variables to pass to the subroutine

- **ICIRunEventRuleActionParams**class is added implementing **ICIRunEventRuleActionParams**interface
- Create and configure action set action:

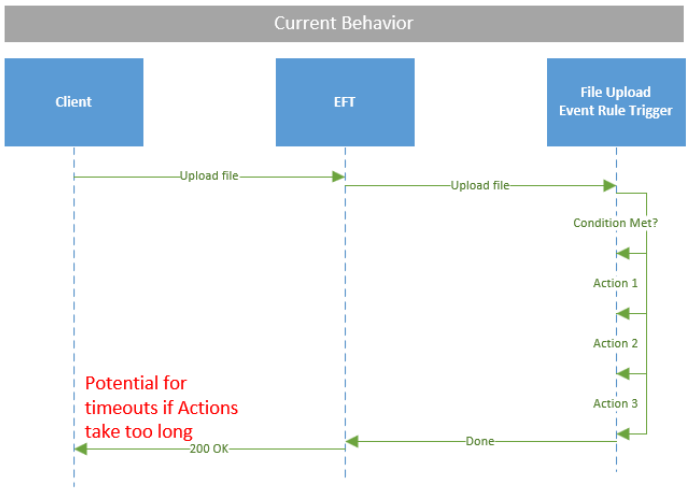
```
Params = CreateObject
("SFTPCOMInterface.CIRunEventRuleActionParams")
 actionParams.RuleName = "Event Rule Subroutine"
actionParams.Variables
 = Array("VAR1", "VAR2", "VAR3") rule.AddActionStatement
 0, actionParams
```

- Read action:

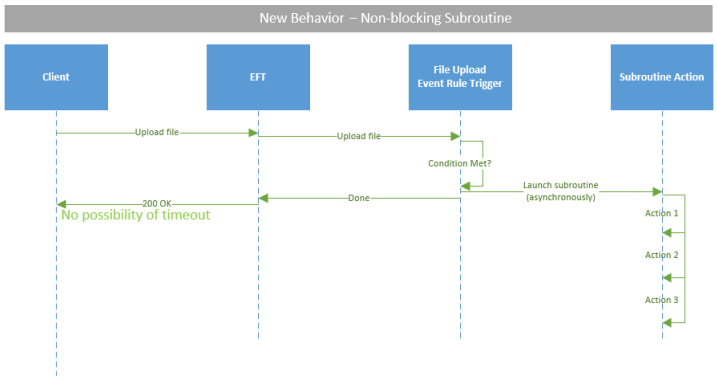
```
set params = action.GetParams()
 MsgBox "Rule name: " & params.RuleName for each var in
params.Variables
 MsgBox "Variables: " & var next
```

EFT Subroutine Action Behavior

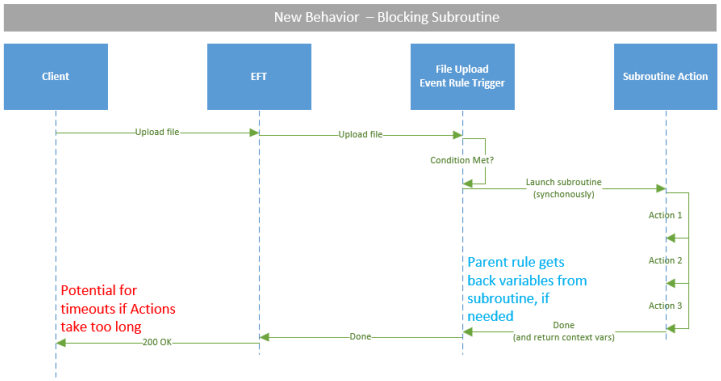
While the primary purpose of the Subroutine action is to help you break up larger rules into smaller, reusable ones, there is an additional benefit. Without the Subroutine action, rules triggered by file uploads do not return a positive completion reply to the remote client until after all actions in the rule have completed, which results in an increased risk of a client time out:



By adding a subroutine action, you can instruct the rule triggered by the upload to call a subroutine in a non-blocking (asynchronous) manner, which allows the upload rule to return the positive completion reply much sooner, mitigating the risk of timeouts:



If desired, subroutines can be called in a blocking (synchronous) fashion which, while increasing the chance of client timeouts, is useful when the parent action needs a result from the subroutine to properly complete its task:



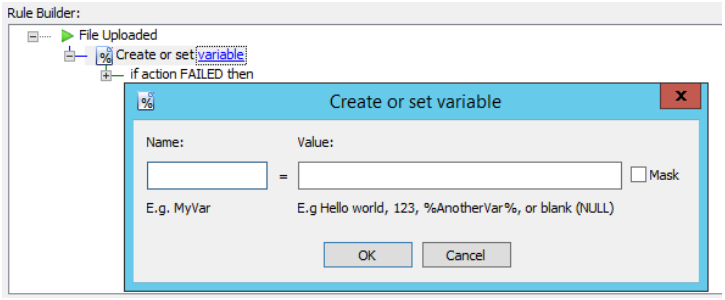
Flow: Variable Action

The **Flow: Variable** Action is used to create or modify a variable to be used in Event Rules. This Action can be used in any events in EFT.

If you attempt to create a new variable with the same name as an existing variable, the existing variable is overwritten and a new variable is not created.

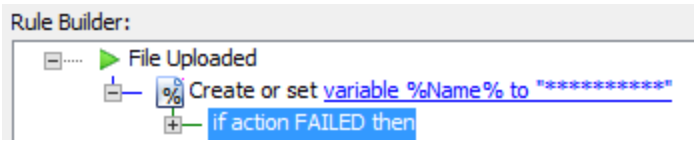
To create a variable in a rule

1. In the administration interface, connect to EFT and click the **Server**tab.
2. Create a new Event Rule.
3. Add the **Create or set variable** Action to the rule.
4. In the Rule Builder, click the **variable**link. The **Create or set variable**dialog box appears.

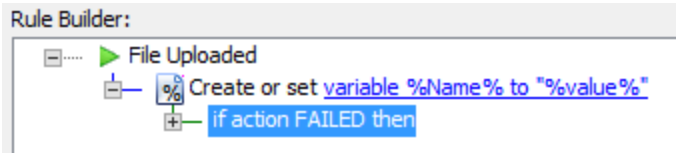


5. Provide a **Name**for the variable:
   - You can specify any character besides the percent sign (%); however, it is recommended to use uppercase and lowercase letters and numbers
   - EFT automatically handles the % whether or not % symbol is provided for variable name
   - Reserved names (other context variables) are allowed. This will overwrite their existing values.
   - Variable names are case sensitive
6. Provide a **Value**for the variable:
   - The value can be blank (NULL), a value, or another variable. You can specify multiple variables, and existing EFT variables. The existing variable's value will be overwritten when this action is triggered.
   - A blank value equals to NULL (NULL not "NULL")
   - EFT will perform casting (converting the variable to its value), as it does today
   - Another variable can be used (passed by reference, not as a pointer)

7. If you want the value to be hidden, select the **Mask** check box. Masked values are replaced with asterisks (**********) in interfaces. On export, values are exported in hex.

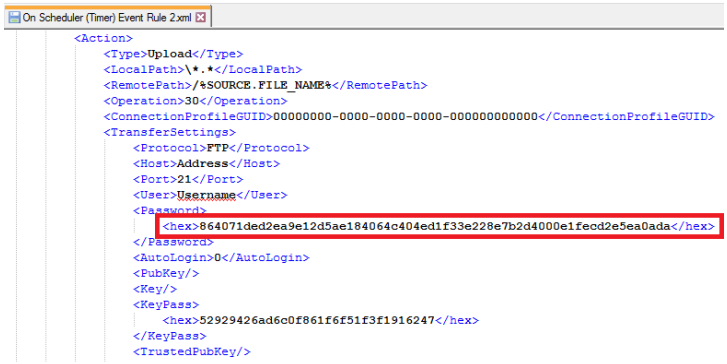


8. Click **OK** to save the **Create or set variable**Action in the rule. The rule in the Rule Builder updates to show your variable definition:



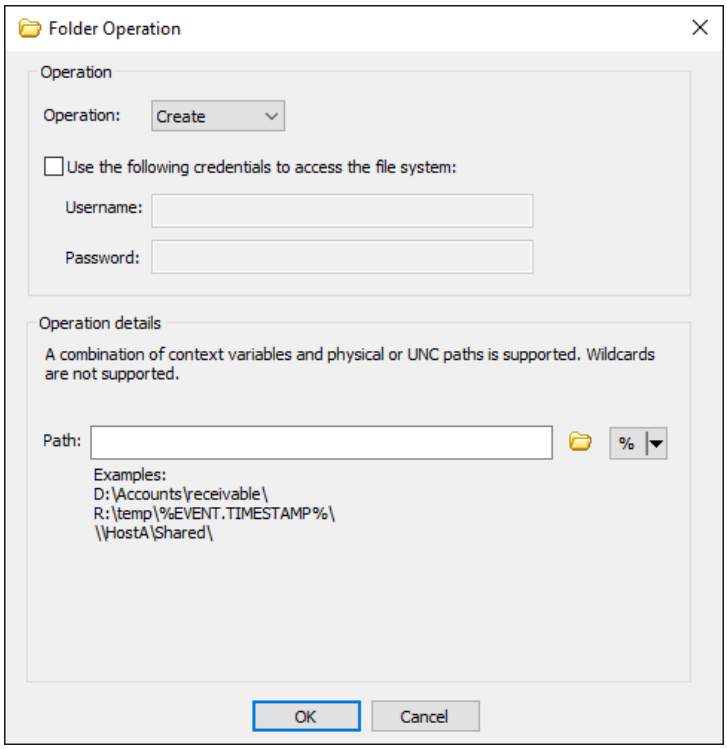
9. Add other conditions or actions as needed, then click **Apply** to save the rule.

Variables are masked in interfaces and in export files:



Folder: Operation Action

(Require EAM) The **Folder: Operation** Action is used to create, rename, or delete a folder.



To create, rename, or delete a folder

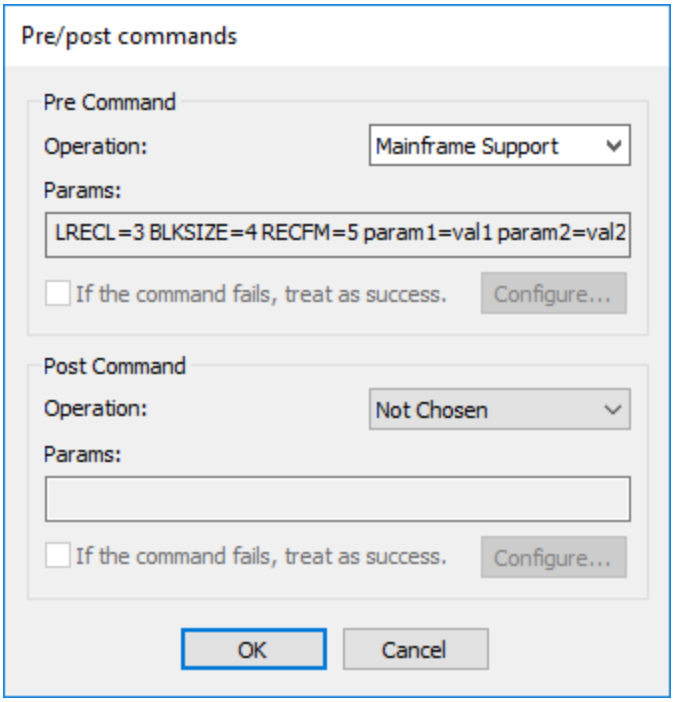
1. Add the **Folder: Operation**Action to the rule, then click the link in the rule to open the **Folder Action** dialog box.
2. In the **Operation**list, click **Create**, **Rename**, or **Delete**.
3. Select the **Use the following credentials to access the file system** check box, then provide the username and password needed to log in to create, rename, or delete the folder.
4. In the **Path**box, provide the path where the folder is that you want to delete, or the location of the folder that you want to create or rename. You can use physical or UNC paths, but not wildcards. You an also click the folder icon to browse to a path, and click the **%**drop-down to add a variable.
5. Click **OK** to save the Action.

Pre and Post Commands

(Requires FTC module) When connecting to a mainframe for file transfers, you might need to provide specific parameters in the Protocol: Upload Action and Protocol: Download Action.

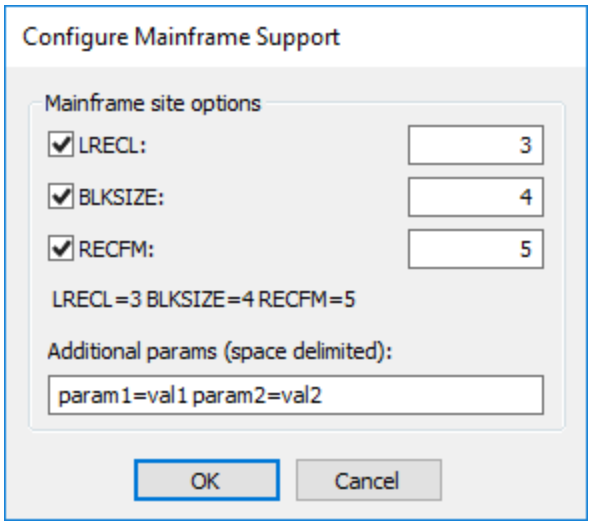
To define commands to occur before and after the upload or download action

1. When defining the **File Offload Configuration** or **File Download Configuration** to connect to a mainframe computer, click **Pre/Post**.



2. In the **Pre/post commands**dialog box, click the **Operations** drop-down list to specify one of the following operations to occur before and after the Upload Action.
    - Not Chosen
    - Create Folder
    - Remove Folder
    - Rename Folder
    - Delete File
    - Mainframe Support - Used to specify information that may be required when sending a file/dataset to a mainframe computer.

3. For the Upload action, in the **Params** box, you can specify any other necessary parameters that need to be passed.
4. Select the **If the command fails, treat as success** check box if you want the event rule to continue.
5. When you choose the **Mainframe Support** operation, then click **Configure**, the **Configure Mainframe Support**dialog box appears.



6. Select the applicable check boxes and provide the parameters:
   - **LRECL**= Logical Record Length; By default, Windows creates files with a logical record length of 256, at which point the line wraps. You can specify a different length in this box.
   - **BLKSIZE**= Block Size of the data set; Normally a multiple of LRCEL.
   - **RECFM**= Record Format; Specifies the characteristics of the records in the data set as:
     - F - Fixed record length
     - V - Variable record length
     - U - Undefined record length
     - B - Blocked records
     - S - Spanned records
     - A - Records contain ISO/ANSI control characters
     - M - Records contain machine code control characters

   For the Upload action, the **Additional params** box can be used to provide other parameters as needed. Separate multiple parameters with a space (not a comma).

7. Click **OK** to save the Pre/post commands configuration.

Datasets in Event Rules

You can create and interact with a dataset using Event Rules dataset Actions.

The data in a dataset is laid out like a database table, which has a unique name and consists of columns and rows. The columns consist of pre-defined units of data. The rows contain the actual data for the columns. An example of a simple dataset containing customer data is illustrated below. The name of the dataset is Customers. The first row (in bold) contains the unique names of the dataset columns, which in this case, describes the data type. All other rows include the actual data as described by each column.

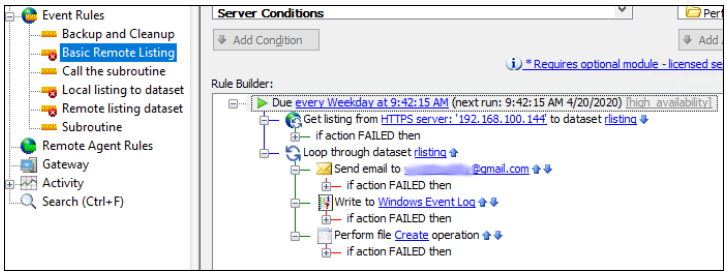
Datasets are accessed in the same way that you access information in a database, by specifying the column and row where the data resides. Every dataset created and used must have a unique name. The unique name of the dataset must be referenced followed by the column name enclosed in percentage signs. For example: `%DatasetName.ColumnName%`

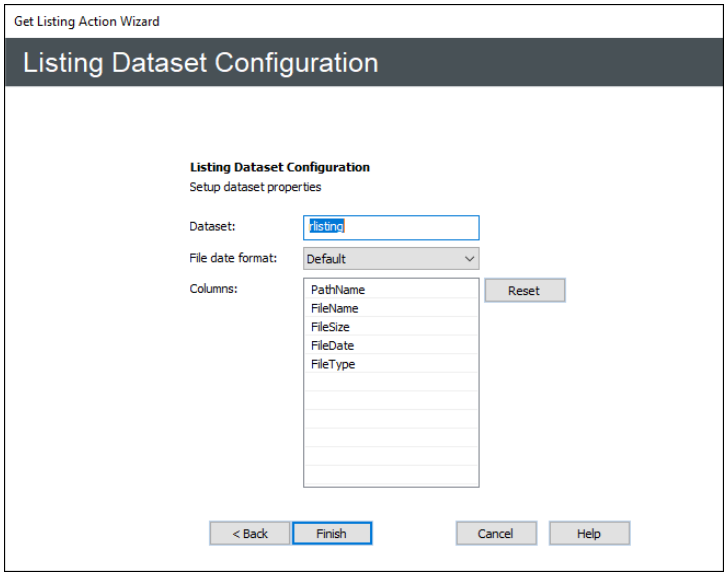
When a dataset is created, the current row is automatically set to 1 (assuming that the dataset has any data, since it is possible for a dataset to have 0 rows, such as when a SQL Query returns no data). A dataset is of minimal use, however, unless one can access the other rows. Typically, this is accomplished by using the Loop through Dataset action, which takes a dataset name as a parameter and automatically increments the current row with each iteration. The loop continues until all the rows have been accessed. In this way, you could make a task that performs operations on each row of the dataset while using the same expression. For example: `%Customers.Email%.`

Using a Loop through Dataset Action is not the only way to access dataset rows. It is possible to directly access a particular row of a dataset by supplying the row number within the expression. For example, if the dataset contains five rows and you need to get the data in row 2, simply enter the row number enclosed in parenthesis directly after the dataset name. For example: `%DatasetName(2).ColumnName%.`

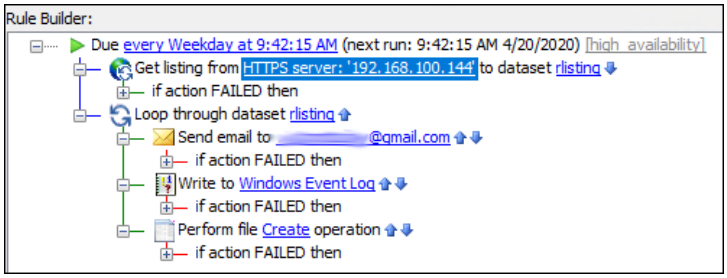
Example of creating and using a dataset in Event Rules

Create an Event Rule to connect to a remote EFT, login as that remote user, grab the contents of the user's home directory, and pipe it out to a dataset. You can list to the dataset over any protocol, HTTPS, SFTP, FTPS



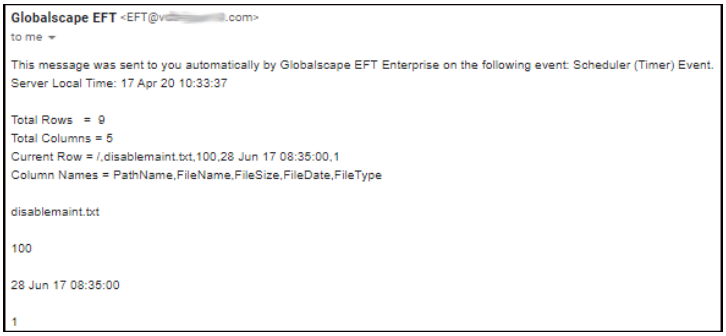


You can take the contents of that dataset and output the contents via Email, Windows Event Log, or write to a file.

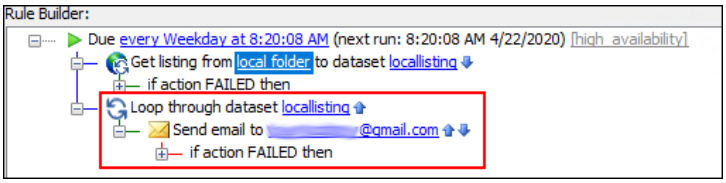


Below is an example of what contents you need to put in the Email, WEL, or file write to grab the contents:

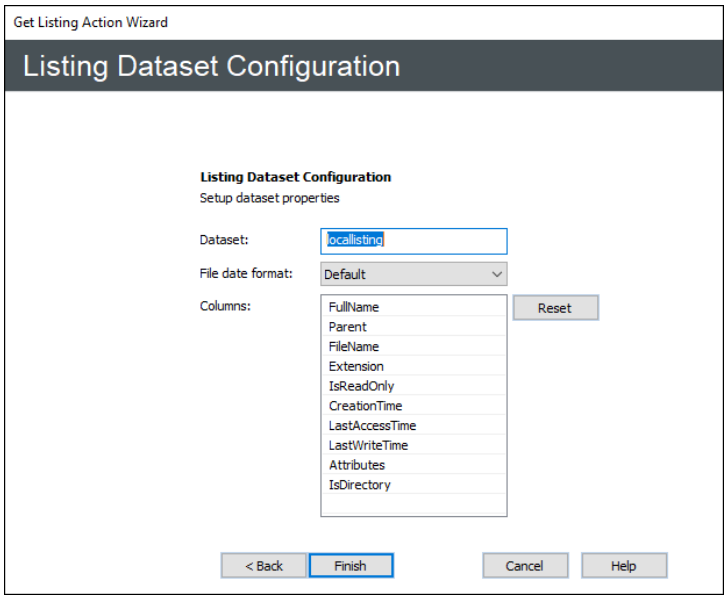
```
Total Rows    =  %rlisting.TotalRows%
Total Columns = %rlisting.TotalColumns%
Current Row = %rlisting.CurrentRow%
Column Names = %rlisting.ColumnNames%
%rlisting.CurrentRow.FileName%
%rlisting.CurrentRow.FileSize%
%rlisting.CurrentRow.FileDate%
%rlisting.CurrentRow.FileType%
```



Local listing to dataset



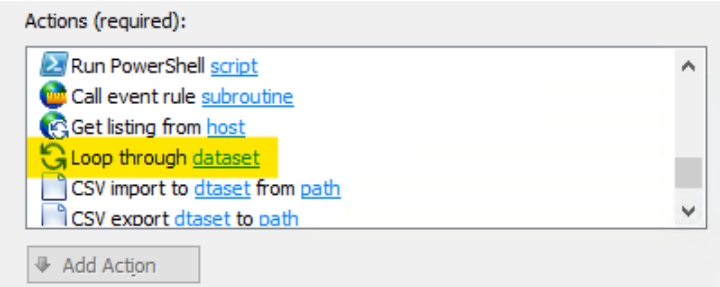
Get Listing from Host Action



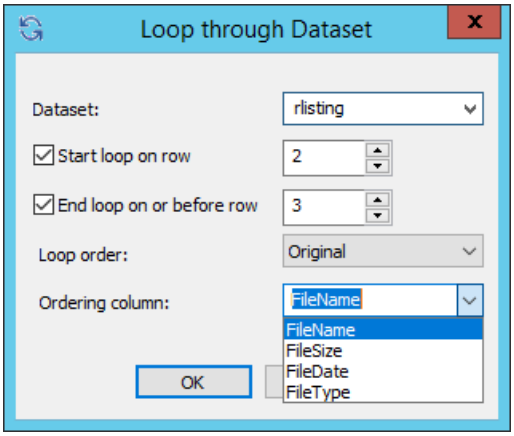
Below is an example of what contents you need to put in the Email, WEL, or file write to grab the contents of the local listing:

```
Total Rows   =  %locallisting.TotalRows%
Total Columns = %locallisting.TotalColumns%
Current Row = %locallisting.CurrentRow%
Column Names = %locallisting.ColumnNames%
Full Name = %locallisting.CurrentRow.FullName%
Parent = %locallisting.CurrentRow.Parent%
File Name = %locallisting.CurrentRow.FileName%
Extension = %locallisting.CurrentRow.Extension%
Is Read Only = %locallisting.CurrentRow.IsReadOnly%
Creation Time = %locallisting.CurrentRow.CreationTime%
Last Access Time = %locallisting.CurrentRow.LastAccessTime%
Last Write Time = %locallisting.CurrentRow.LastWriteTime%
Attributes = %locallisting.CurrentRow.Attributes%
Is Directory = %locallisting.CurrentRow.IsDirectory%
```

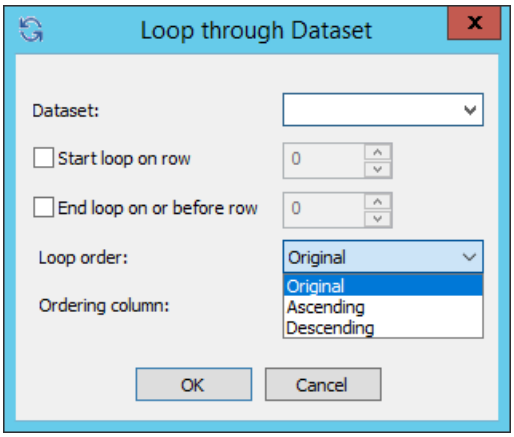
Loop Through Dataset Action



You can specify to loop through the whole dataset, or start and end on a specific row, and specify the column for ordering.



You can specify the order of the loop to start from its Original order, or specify an Ascending or Descending order.

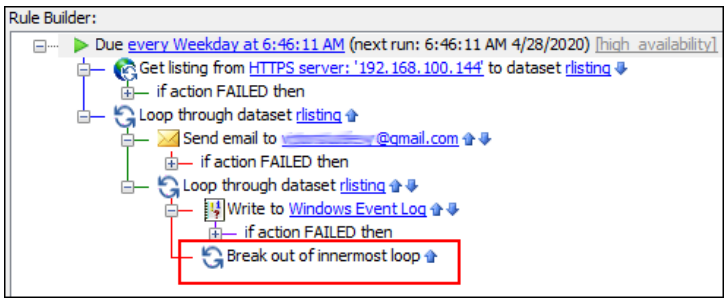


Loops can also be added into other loops

In this event rule, for each cycle of the external loop it will perform an internal loop:

Break from loop

When conditions in the loop are met, there is no need to continue parsing the dataset. In this event rule, the second loop will break after it runs through the dataset one time. The first loop will continue until complete.



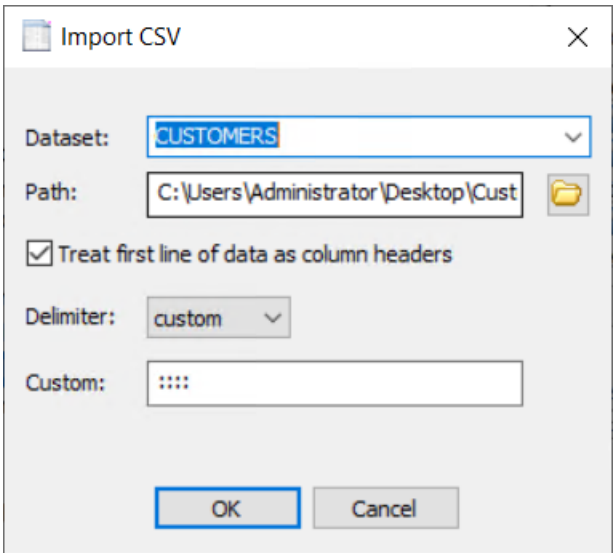
CSV Export/Import to Dataset to/from Path

You can import data from a CSV file into a dataset, so that you can later import that work with this dataset in EFT's rules (loop through dataset for example)

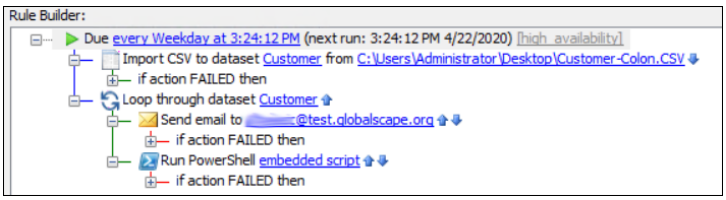
In the **CSV import to dataset**dialog box is used to specify the source CSV file (Click the file icon and click the file that you want to import). In this way, you can create and populate a dataset. Advanced options allow you to treat the first line of data as column headers and specify the delimiter format (comma, semicolon, tab, space, or custom). Comma is the default.

If the option "Treat first line of data as column headers" is not selected, the dot notation for referencing the `fields in a records will be: Column0, Column1, Column2, and so on.`

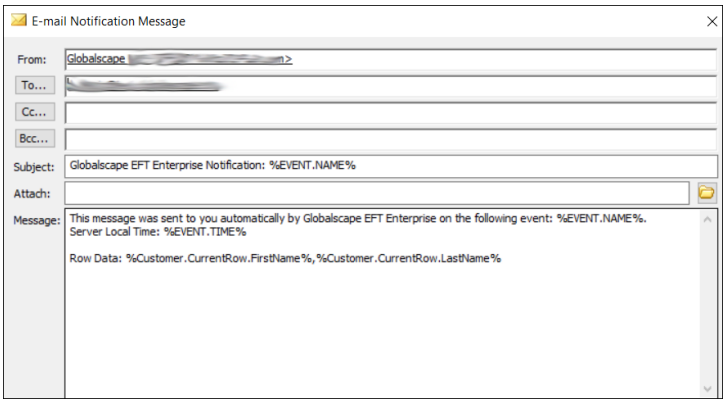
For the record below it would be `%Customer.CurrentRow.Column0%`.



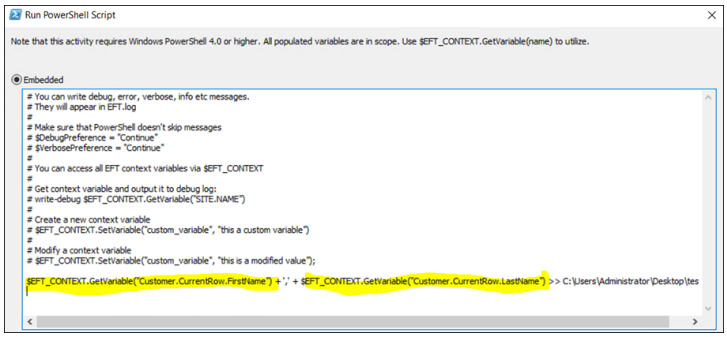
You can create an Event Rule that reads in a CSV-formatted file and then uses the records in the dataset in the steps of the Event Rule:



Referencing the dataset in dot notation will look like this in the **Send notification email** Action:

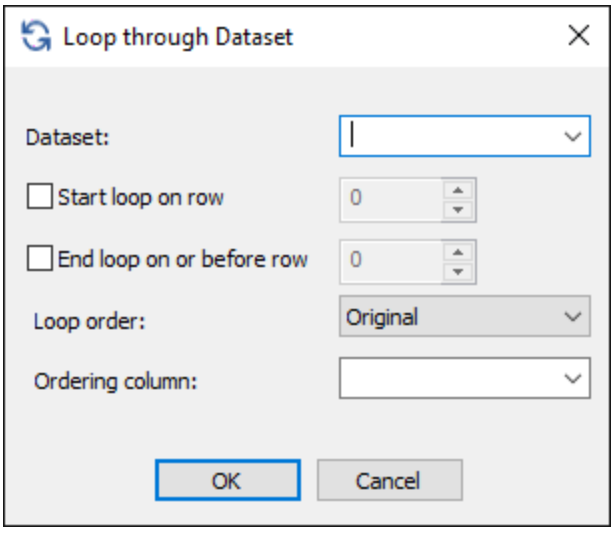


PowerShell does not handle the % sign. The example below shows how to reference custom variables:


Run PowerShell Script
Note that this activity requires Windows PowerShell 4.0 or higher. All populated variables are in scope. Use $EFT_CONTEXT.GetVariable(name) to utilize.
Embedded
You can write debug, error, verbose, info etc messages.
They will appear in EFT.log
#
Make sure that PowerShell doesn't skip messages
$DebugPreference = "Continue"
$VerbosePreference = "Continue"
#
You can access all EFT context variables via $EFT_CONTEXT
#
Get context variable and output it to debug log:
write-debug $EFT_CONTEXT.GetVariable("SITE.NAME")
#
Create a new context variable
$EFT_CONTEXT.SetVariable("custom_variable", "this a custom variable")
#
Modify a context variable
$EFT_CONTEXT.SetVariable("custom_variable", "this is a modified value");
$EFT_CONTEXT.GetVariable("Customer.CurrentRow.FirstName") + ',' + $EFT_CONTEXT.GetVariable("Customer.CurrentRow.LastName") >> C:\Users\Administrator\Desktop\tes

Loop: Dataset and Loop Break Action

(Require EAM) A **Loop: Dataset** Action reads through ("parses") a dataset until the end of the dataset is reached or a Loop Break is used to stop the loop.

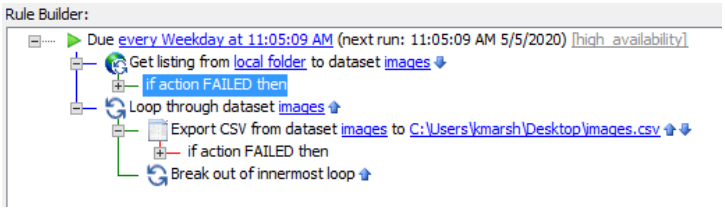


- You can specify to loop through the whole dataset, or start and end on a specific row.
- You can specify the order of the loop to start from its original order, or specify an Ascending or Descending order.
- You can specify the **Ordering column** for the loop. The default is the first column.
- Loops can also be added into other loops (see example provided below).
- Loop break action is not available outside of a loop statement and is not visible when selecting event rule. Also, you can't move a Loop Break out of the most outer loop in the Rule Builder using drag & drop.

Loop Break

The Loop Break Action is only displayed when it is usable. You can break from a loop when conditions are met earlier in the loop and there is no need to continue parsing the dataset.

In this Rule, the second loop will break after it runs through the dataset 1 time. The first loop will continue until complete.



Dataset size is limited to 10,000 rows to avoid out-of-memory crashes.

Related Topics

- Protocol: Listing to Dataset Action
- CSV Export-Import to-from Dataset

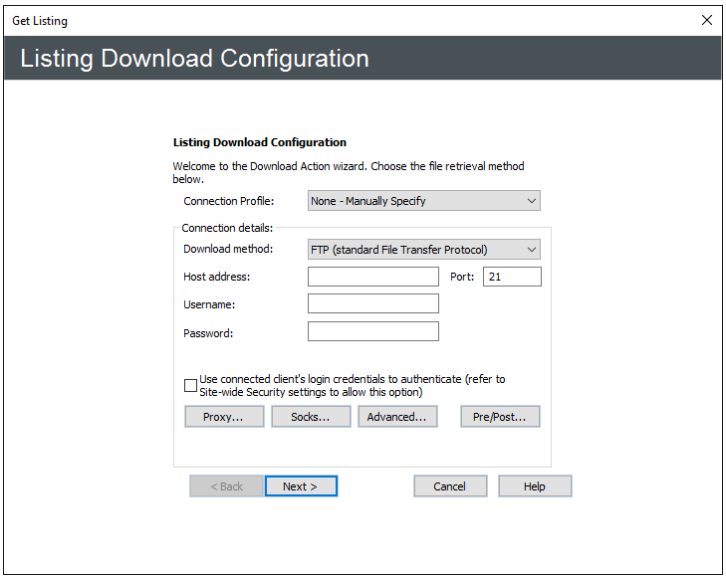
Protocol: Listing to Dataset Action

(Require EAM) The **Protocol: Listing to Dataset**Action is used to read from a remote directory listing to create a dataset or read from a CSV file to create a dataset.

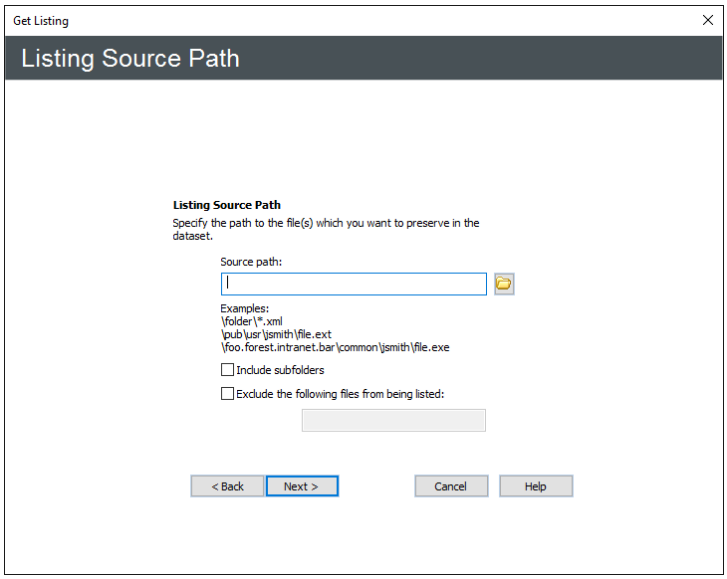
> **NOTE:** Dataset size is limited to 10,000 rows to avoid out-of-memory crashes.

To create the dataset

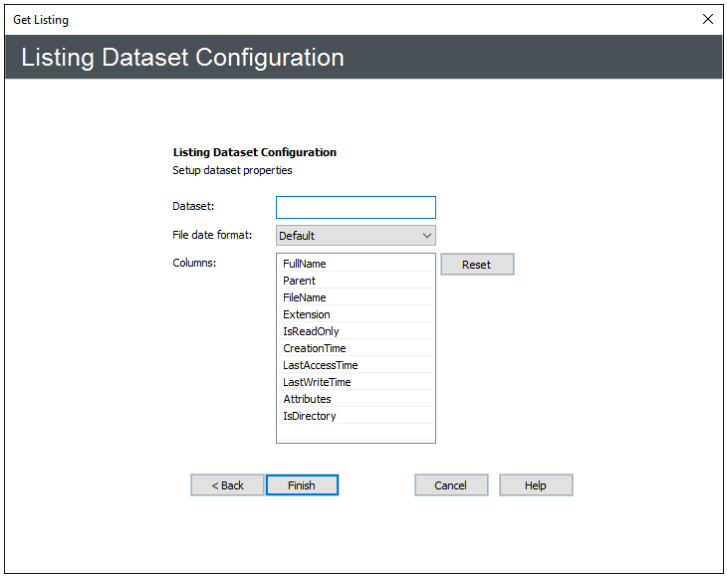
1. Create an Event Ruleusing the Scheduler (Timer) Event.
2. Add the **Get listing from host**Action to the Rule.
3. Click the server link to open the **Get Listing Action** wizard.
4. Specify the **Connection**details. (See Download Action for details, if needed.)



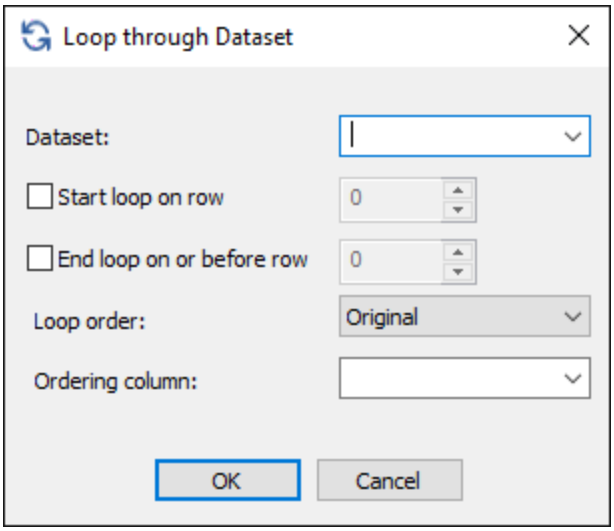
5. Specify the **Source path** (See DownloadAction for details, if needed).



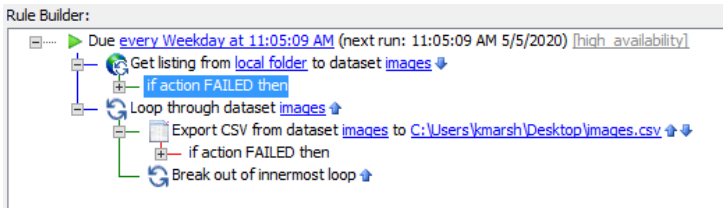
6. Specify the **Dataset properties.**



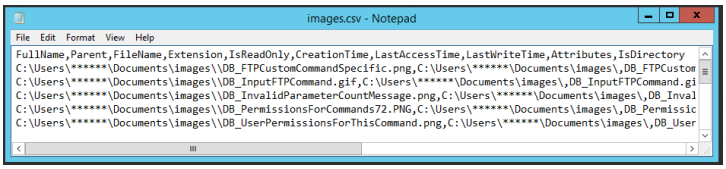
7. The **Dataset** can name can be whatever you want.
8. The **File date format**can be **Default**, **Epoch**, or **ISO-8601**.
9. The **Columns** are based on the directory you're pointing to.
10. Click **Finish** to close the wizard.
11. Add the **Loop through dataset**Action, and specify the Loop properties. (Refer to Loop Through Dataset Action for more information, if needed.)



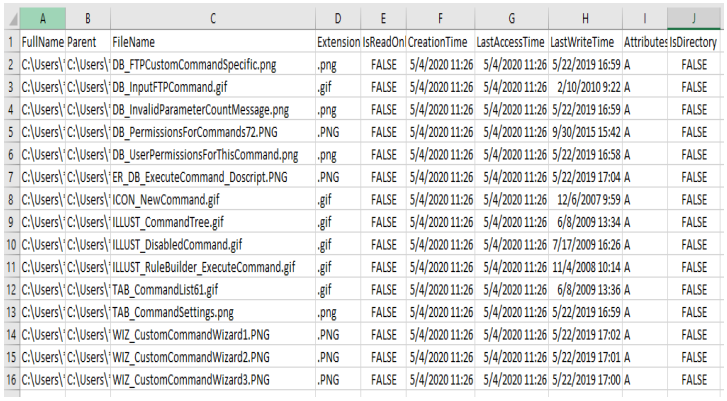
12. The **Dataset** name that you specified in the **Get Listing Action** wizard appears as a selection in the **Dataset**drop-down list..
13. The column names from the **Get Listing Action** wizard appear in the **Ordering column** drop-down list.
14. Click **OK**.
15. Add an Action for what to do with the data, such as the CSV export dataset to path Action.



16. Using the **CSV export dataset to path** Action, the output looks similar to this:



17. Which you can then open as a spreadsheet:



	A	B	C	D	E	F	G	H	I	J
1	FullName	Parent	FileName	Extension	IsReadOn	CreationTime	LastAccessTime	LastWriteTime	Attributes	IsDirectory
2	C:\Users\	C:\Users\	DB_FTPCustomCommandSpecific.png	.png	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 16:59	A	FALSE
3	C:\Users\	C:\Users\	DB_InputFTPCommand.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	2/10/2010 9:22	A	FALSE
4	C:\Users\	C:\Users\	DB_InvalidParameterCountMessage.png	.png	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 16:59	A	FALSE
5	C:\Users\	C:\Users\	DB_PermissionsForCommands72.PNG	.PNG	FALSE	5/4/2020 11:26	5/4/2020 11:26	9/30/2015 15:42	A	FALSE
6	C:\Users\	C:\Users\	DB_UserPermissionsForThisCommand.png	.png	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 16:58	A	FALSE
7	C:\Users\	C:\Users\	ER_DB_ExecuteCommand_Doscript.PNG	.PNG	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 17:04	A	FALSE
8	C:\Users\	C:\Users\	ICON_NewCommand.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	12/6/2007 9:59	A	FALSE
9	C:\Users\	C:\Users\	ILLUST_CommandTree.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	6/8/2009 13:34	A	FALSE
10	C:\Users\	C:\Users\	ILLUST_DisabledCommand.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	7/17/2009 16:26	A	FALSE
11	C:\Users\	C:\Users\	ILLUST_RuleBuilder_ExecuteCommand.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	11/4/2008 10:14	A	FALSE
12	C:\Users\	C:\Users\	TAB_CommandList61.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	6/8/2009 13:36	A	FALSE
13	C:\Users\	C:\Users\	TAB_CommandSettings.png	.png	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 16:59	A	FALSE
14	C:\Users\	C:\Users\	WIZ_CustomCommandWizard1.PNG	.PNG	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 17:02	A	FALSE
15	C:\Users\	C:\Users\	WIZ_CustomCommandWizard2.PNG	.PNG	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 17:01	A	FALSE
16	C:\Users\	C:\Users\	WIZ_CustomCommandWizard3.PNG	.PNG	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 17:00	A	FALSE

Related Topics

- Loop: Dataset Action
- CSV Export-Import to-from Dataset

Protocol: AS2 Action

(Requires AS2 module) The topics in this section provide instructions for administering the AS2 action.

- Protocol: AS2 Action - Sending Files to an AS2 Partner via Event Rules
- AS2 Information in the Database
- AS2 Transaction Reports
- Transfers - AS2 Status Viewer
- Resubmitting AS2 Transmissions
- AS2 Transaction Success and Failure Notification

Sending Files to an AS2 Partner via Event Rules

(Requires AS2 module) You can send files via AS2 to a partner for whom you have not previously provisioned an outbound profile by manually specifying that partner's profile in the **AS2 Send File** Event Rule Action. Alternatively, if the AS2 partner has an outbound profile defined, you can select that profile when you define the **AS2 Send File** options.

For example, you could define a Rule with a Timer Event so that every Monday at 8 a.m., all files in a certain folder are sent either to a partner that already has a profile defined on the Server or to a partner that you will define "on the fly" in the **AS2 Send File** dialog box.

The **AS2 Send File to host** Action can be used for Folder Monitor, Timer, and all file-based Events.

UTF-8 filenames/non-ASCII characters are not supported over the AS2 protocol. It is the responsibility of the trading partners to determine the file-naming limits imposed by their trading environments. Refer to RFC 2183, section 2.3 for details of filename parameters.

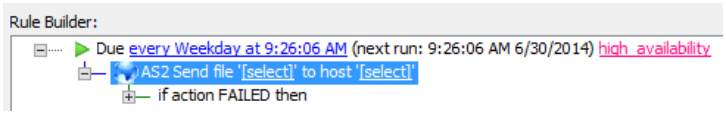
When triggered, the **AS2 Send File to host** Action offloads one or more user-defined files or one or more context files. Depending on the **AS2 Send File to host**Action's retry configuration, the Action fails if any error occurs when attempting to send the AS2 payload. Those errors may include any connection, authentication, transport, or navigation errors; receipting errors or failures; payload errors, including transfer errors or integrity mismatch errors or failures; server communicated errors; and unknown or undefined errors, such as:

- No receipt was provided
- The receipt was not signed
- The MIC value returned did not match the original file/message MIC
- EFT was unable to:
    - verify the receipt signature
    - establish a connection to the remote host
    - upload the file to the remote host
    - send an the receipt asynchronously
    - send the receipt synchronously

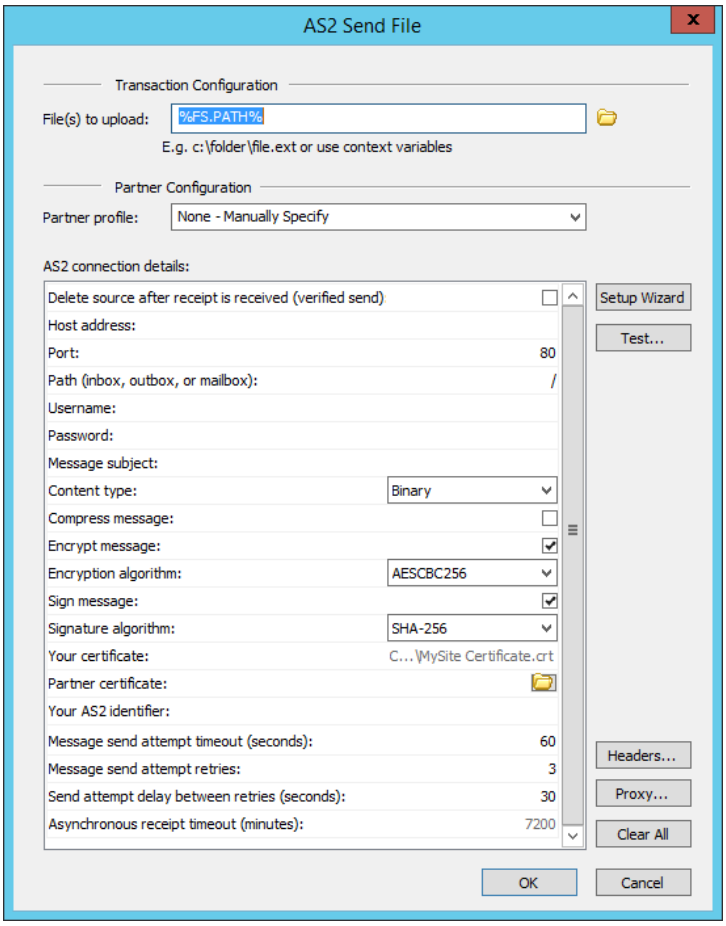
To send files using the AS2 Send File to host Action

1. Create a new Event Rule, such as a Scheduler (Timer) Event. (Refer to Creating Event Rules for details of creating Event Rules, if necessary.)

2. Add the **AS2 Send file to host** Action to the Rule.



3. Click one of the underlined text links. The **AS2 Send File** dialog box appears.



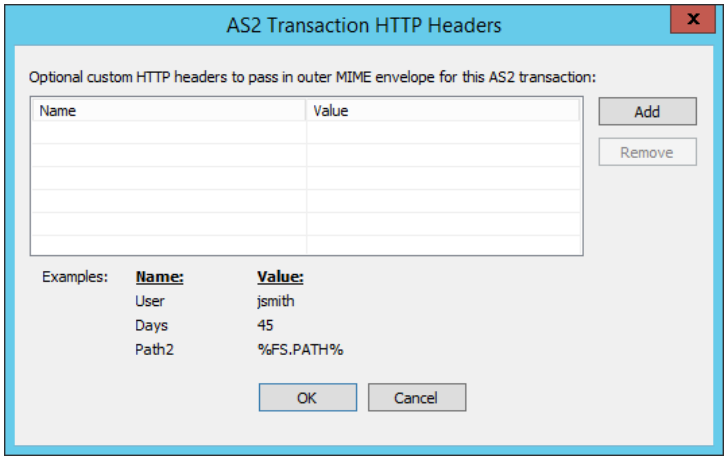
4. In the **File(s) to upload** box, type the path or click the folder icon to specify the file to send to this partner. Include the entire path to the file. You can also use File System context variables such as %FS.PATH% or wildcard masks. For example, to send all files in a folder, type the folder path and ***.***. (The files will not be sent all at once; each file will have a unique message ID.)
5. In the **Partner Configuration** area, specify the AS2 Partner profile using one of the following methods:
    - In the **Partner profile** box, select a defined AS2 outbound partner profile. The fields in the **AS2 connection details** area is completed automatically.

- Provide the connection details in the **AS2 connection details** area. (Refer to AS2 Send File Dialog Box Fields below for details of each field.)
- Click **Setup Wizard** to use the wizard to set up the profile.

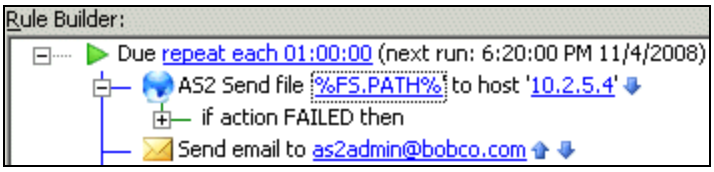
  The **Partner profile** box is linked to the selected profile configuration. If you are using Globalscape authentication, if the profile is updated, the information in the **AS2 Send File** dialog box is updated also; if a referenced profile is deleted, disabled, or not allowed to use AS2, any Event Rule using the profile will fail.

  When you use AD, LDAP, or ODBC authenticated accounts as AS2 partners, if the account in the external database is changed, deleted, or disabled, any Event Rule or Command that references the account will fail. For example, if an AD user SSmith is renamed SJones, you will have to update any Event Rule or Command manually to reflect the new name of the account.

6. To test the configuration, click **Test.**
7. (Optional) Click **Headers**to add a custom header. The purpose of custom HTTP headers is to pass additional or required information to the recipient's server. The **Name** and **Value** fields can each contain up to 255 characters. The **Value** field can use context variables.



   - To add the header, click **Add**, then provide the name and value in the table, as shown in the examples in the dialog box.
8. To configure a proxy server for this partner, click **Proxy**.
9. To clear all of the partner connection details and start over, click **Clear All**.
10. Click **OK** to save the AS2 Partner profile in the Event Rule.
11. Add other Conditions and/or Actions, as needed (for example, add an email notification).



12. Click **Apply** to save the Event Rule on EFT.

AS2 Send File Dialog Box Fields

The AS2 Send File dialog box can be used in Folder Monitor, Timer, and file-based Event Rules. The table below describes each field in the **AS2 Send File** dialog box.

Field	Required/Optional	Description
File(s) to upload	Optional	Used to specify the file(s) to upload to the partner. Can be variables or paths. e.g. **c:\temp\robert.txt** or (if relative path) **\rob.txt**Defaults to %FS.FILE_NAME%; same as if blank. Accepts FS.FILE variables and path strings to drive or UNC paths or relative path where applicable (for example, if using a Folder Monitor Rule).
Partner profile	Required	Used to select a defined partner profile or left blank (the default) if the partner profile is not defined. If blank, complete the fields in the **AS2 Partner profile** area.
Delete source	Required	Used to indicate whether to delete sources files after sending them to the destination, after the MDN is received and verified from the remote AS2 host. Select the check box to delete source files after the MDN is received and verified from the remote AS2 host.
Host address	Required	AS2 outbound host address. **Requires protocol prefix in URL (http:// or https://).** Specified in **AS2 Partner Access** wizard.
Port	Required	AS2 Outbound port. Range is 1-65K
Path (inbox, outbox, or mailbox)	Optional	Relative path (similar to User Home Folder); forward slash (/) by default
Username	Optional	User login name
Password	Optional	Password
Message subject	Optional	AS2 message subject

Field	Required/Optional	Description
Content type	Required	AS2 content type. Options include: • **X12** - Format used by many healthcare, insurance, government, transportation, and finance organizations. • **EDIFACT** - Format adopted by the International Organization for Standardization (ISO) as the ISO standard ISO 9735. • **XML** - File format used for structured documents. • **EDI Consent** - Provides a standard mechanism for "wrapping" the EDI objects but does not specify any details about those objects. • **Binary** (default) - e.g., executables, word processing files, database, spreadsheet, and multimedia files • **Plaintext** - e.g., text and HTML files
Compress message	Required	When selected, specifies that the AS2 message should be compressed when sent. (Cleared by default.)
Encrypt message	Required	When selected, specifies that outbound AS2 messages should be encrypted. (Selected by default.)
Sign message	Required	When selected, specifies that outbound AS2 messages should be signed. (Selected by default.)
Your certificate	Required	Displays the AS2 certificate public key path to use for signing, copied from the Site. (Can be on a drive or UNC path.)
Partner certificate	Required	Specifies the AS2 certificate to use for encrypting outbound transactions and for validating signed MDN receipts. (Can be on a drive or UNC path.)
Your AS2 identifier	Required	Used to apply a unique **AS2-From** ID to outbound messages.
Partner AS2 identifier	Required	Used to apply a unique **AS2-To** ID to outbound messages.
Receipt policy	Required	Used to request an MDN receipt. Options include: • Request a signed receipt (default) • Don’t request a receipt • Request an unsigned receipt
Receipt delivery	Required	Specifies receipt delivery method: Synchronous (default) or Asynchronous Asynchronous receipts will be returned to the domain name specified on the Site's **Connection** tab using the standard or secure listener port specified on that same page (depending on whether you specified HTTP or HTTPS for the remote host value).

The following fields are used to determine whether a message send attempt has failed due to a timeout, error, synchronous MDN receipt failure, or other error, after which EFT will attempt to resend the same message at regular intervals, if specified.

Field	Required/Optional	Description
Message send attempt timeout (seconds)	Optional	Specifies the timeout after which a message send attempt is considered a failure if no response or errors are received from the remote server. Range: 0-600, 60 by default, 0 means no timeout
Message send attempt retries	Optional	Number of times to reattempt to send the message. Range: 0 (no retry) to 999, 10 is the default. Retries do not include the initial attempt. That is, 3 retries means 3 in addition to the first attempt (4 total).
Send attempt delay between retries	Optional	Specifies the time to wait between retries if the send attempt was unsuccessful, in seconds. 30 seconds is the default.
Asynchronous receipt timeout	Optional	Specifies the time to wait for receipt before timing out, in minutes. The default is 7200 minutes (2 hours).

AS2 Information in the Database

(Requires AS2 and HTTP/S module) The Auditing and Reporting module (ARM) is not required, but is recommended for auditing purposes. (The receipt policy is not dependent on ARM.) EFT provides a sub-node on the **Status** tab that displays a history of AS2 transactions.

The following information is audited to the ARM database:

- Date/Time
- Raw HTTP Headers
- File name
- MDN
- MIC*
- Content Type
- Message-ID
- Remote/Local File path (mailbox)
- Remote/Local Host (hidden by default)
- Status: Success (S), Failure (F), or In Progress (IP)
- Direction: Inbound or Outbound
- EFT AS2 ID
- Partner AS2 ID
- Error (only if Failure) occurred, the verbose error. Otherwise "None".
- Action:
  - Inbound Connection (S, F, IP)
  - Outbound Connection (S, F, IP)
  - Receive File (S, F, IP)
  - Send File (S, F, IP)
  - Send Receipt Asynchronous (S,F,IP)
  - Send Receipt Synchronous (S,F,IP)
  - Receive Receipt (S,F, IP)
  - Receipt Verification (S,F)

*EFT calculates the AS2 MIC using SHA-1. (Refer to RFC 3335 for details.) You can ignore the words "MD5" that appear in the MIC column of the AS2-related reports (**tbl_AS2Transactions** column).

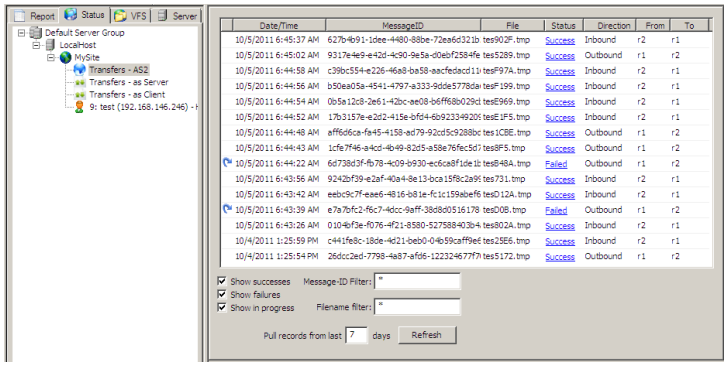
AS2 Transaction Reports

The Auditing and Reporting module (ARM) gathers AS2 data and provides the data in the Transfers - AS2 node and in predefined AS2 reports. You can also define your own custom reports.

- *AS2 Transactions (Summary)* report - A transaction report that displays more detailed information than what is shown on the **Transfers – AS2** node. The report queries all AS2 transactions for the dates specified, grouped by Site, sorted by date, and listed in reverse chronological order. You can add Report Filters for the following data:
  - StartTime
  - MessageID
  - FileName
  - TransactionID
  - FromAS2ID
  - ToAS2ID
  - TransactionStatus (rolled up transaction status)
    - **Success** - File was received/sent MDN successfully received/sent
    - **Failure** - Transaction failed to receive/send after all retries or MDN not received/sent after all retries
    - **In Progress** - Transaction started or is in progress (transferring or waiting for next retry or waiting for MDN, etc.)
- *AS2 Transactions (Detailed)* report - A verbose AS2 file transfer report that provides the information necessary for troubleshooting problem transactions. You can add Report Filters for the following data:
  - StartTime
  - MessageID
  - FileName
  - TransactionID
  - FromAS2ID
  - ToAS2ID
  - TransactionStatus
  - Sitename
  - Error (Displays **None** if there are no errors)

Transfers - AS2 Status Viewer

EFT provides a sub-node on the **Status** tab that displays a history of AS2 transactions.



The **Transfers - AS2** node displays the history of AS2 inbound and outbound transfers, including the result from the MDN. For example, if a file transaction attempt fails 10 times in a row, but succeeds on the 11th attempt and the MDN is sent, the **Transfers - AS2** node reports the transaction as a success. If all of the transaction's file transfer retries fail, then the **Transfers - AS2** node reports the transaction as a failure. If retries are still occurring at the time the **Transfers - AS2** node is invoked, the transaction will be marked as **In Progress**. You can view details of each transaction by clicking its **Status** column. EFT will query and then display (in the default text editor) the details surrounding that transaction as obtained from the ARM database.

When the **Transfers - AS2** node is selected, the last 7 days of transaction summaries are displayed in reverse chronological order. You can change the default of 7 days to display from 1 to 999,999 days of data. Click **Refresh** to display all transactions that may have occurred since the last opening or refresh of the **Transfers - AS2** node.

The node displays the following information:

- **Date and Time** - Last recorded status for the transaction
- **Message ID** - From AS2 header
- **File** - Name of file transferred
- **File Path** - Local inbox or outbox; this column is hidden by default
- **Remote Host Address** - Host address of the sender (Inbound)/receiver (Outbound). This column is hidden by default.
- **Status** - Contains a hyperlink that, when clicked, pulls the *AS2 Detailed* report for that transaction. The report displays transaction details, which is most helpful for in-progress or failed transactions.

  - **Success** - Transaction completed and MDN successfully received/sent
  - **Failure** - Transaction failed to send after all retries or MDN not received/sent
  - **In Progress** - Transaction started or in progress (transferring or waiting for next retry or waiting for MDN, etc.)
- **Direction** - **Inbound** or **Outbound**
- **From** - Server's AS2 ID or the Partner ID (depends on direction)
- **To** - Server's AS2 ID or the Partner ID (depends on direction)

The **Resubmit** icon , to the left of failed transactions, allows you to resubmit the file (s) and/or MDN(s). You can also resubmit a file, or group of files by multi-selecting failed transaction rows, then right-clicking and clicking **Resubmit**. If you resubmit a file that is a part of multi-file transaction, all of the files will be resubmitted. You can only resubmit failed transactions. You cannot resubmit in-progress or successful transactions.

Customizing the Display

You can customize the **Transfers - AS2** status viewer to suit your needs:

- Choose the columns to display or hide by right-clicking on a column header, then selecting/clearing the column name in the submenu.
- Sort by a specific column in ascending or descending order by clicking the column header.
- Define filters to display or hide rows based on **Status**, **Message-ID**, or **File Name**.
  - To filter the display based on status, select or clear the **Show successes**, **Show failures**, and **Show in progress** check boxes, and then click **Refresh**
  - To filter the display based on the message-ID, in the **Message-ID** box, type the message ID, and then click **Refresh**.
  - To filter the display based on the filename, type a name in the **Filename** box, and then click **Refresh**.
  - To change the number of days of history to display, in the **Pull records from last**<*n*>**days** box, type the number of days, from 1 to 9999.
- Refresh or clear the display by right-clicking an empty row, and then clicking **Refresh**, or in the filter area, click **Refresh**.

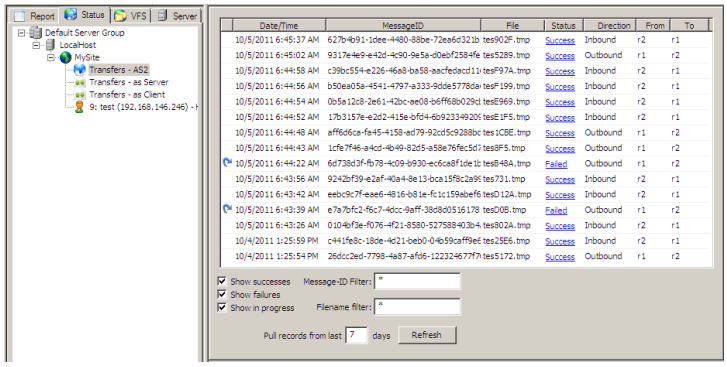
Resubmitting AS2 Transmissions

In the **Transfers - AS2** node, the **Resubmit** icon to the left of failed transactions allows you to resubmit the file(s) and/or MDN(s). You can only resubmit failed transmissions. You cannot resubmit in-progress or successful transmissions.

- **Outbound**. If a failure was an outbound transaction (failed after all retries and the MDN was never received), you can attempt to send the same file again.
- **Inbound**. When an inbound transaction fails, resubmit is allowed only when the failure was due to a failure in sending the receipt (MDN). (EFT cannot resubmit the file, because it did not send it to begin with.) The resubmit action attempts to resend the MDN receipt.

To resubmit a transmission

1. In the administration interface, connect to EFT, and click the **Status** tab.
2. Expand the Server and Site nodes, and then click the **AS2 Transactions** node. The Site's AS2 transactions appear in the right pane.



3. Click in the row of the failed transaction to select it, and then click the **Resubmit** icon . A confirmation prompt appears.
4. Click **Yes**. The transaction is resubmitted and appears in a new row. The resubmitted transaction populates a new row in the **Transfers – AS2** node with the new transaction and new message ID.

   There can be multiple rows (other transmissions) between the failed transmission and the resubmitted transmission.

AS2 Transaction Success and Failure Notification

EFT can execute a command or send an email to notify you of the success or failure of AS2 transactions. The email or Command is triggered when all message send attempts have been attempted or the asynchronous MDN wait time has expired (if applicable).

The email notification and custom command are configured by clicking the applicable link in the **AS2 Inbound** and **AS2 Outbound** tabs or in the AS2 Partner Access wizard.

- Clicking the Transaction FAILED/SUCCESS notification email link, **[Add]**, opens the Edit Mail Template dialog box.
- Clicking the Transaction FAILED/SUCCESS send command link, **[Add]**, opens the Custom Command dialog box. (You will have to define the custom command before using it in the notification.)
- Each of the fields are optional

Field	Description
Transaction FAILED notification email	Opens the **Edit Mail** dialog box in which you can specify an email notification for failed transaction.
Transaction SUCCESS notification email	Opens the **Edit Mail** dialog box in which you can specify an email notification for successful transaction.
Transaction FAILED run command	Opens the **Custom Command** dialog box in which you can specify a **Command**to run upon failed transaction.
Transaction SUCCESS run command	Opens the **Custom Command** dialog box in which you can specify a **Command**to run upon successful transaction.

- Refer to email Notification Action for details of defining an email notification.
- Refer to Creating a Command to create a command and refer to Script: Custom Command Action for details of using a Command.

Related Topics

- Creating a Command
- The Custom Command Wizard
- email Notification Action
- Creating an email Notification Template

Protocol: Download Action

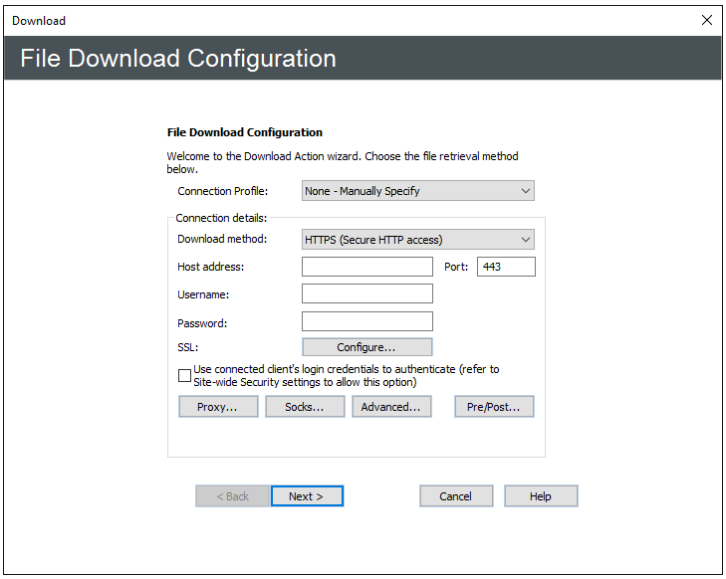
(Requires FTC module) You can configure an Event Rule to copy or download from a specific location to a specified local folder using a particular protocol when an Event occurs. You must provide EFT with connection information (protocol and login details) and file information (source path and destination path). The Download Action is available with all Events except Site Stopped and Service Stopped.

- When you add a **Download file from host** Action to a Rule, the Client FTP offload engine performs retries upon failures (network failures is the typical example) based upon the settings in the **Advanced Options** dialog box. Be aware that the **Download file from host** Action does the transfer, including all retries, before moving on to the next Action, such as an email notification. A long-running transfer that also retries numerous times with large delays will cause the Event Rule to take a long time to complete.
- When setting up the File Download Action using variables, the remote connection test fails because variables appear undefined.

Refer to Connection Profiles for details of setting up a Connection Profile before defining the Action.

To set up EFT to download files

1. Follow the procedure in Creating Event Rules or select the Rule to which you want to add the Action.
2. In the **Actions**list, click **Protocol: Download**. The Rule parameters are added to the Rule in the **Rule Builder**.
3. Click one of the undefined parameters where the parameters are listed in the **Rule Builder**. The **File Download Configuration** wizard appears.



4. In the **Connection Profile** box, specify a connection profile for this Event. If none is specified, you will need to configure the **Connection details** as described below.
5. Click the list to specify a **Download method** for the connection: **Local (Local File or LAN)**, **FTP (standard File Transfer Protocol)**, **FTP SSL/TLS (AUTH TLS)**, **FTP with SSL (Explicit encryption)**, **FTP with SSL (Implicit encryption)**, **SFTP using SSH2 (Secure Shell)**, **HTTP (HyperText Transfer Protocol)**, **HTTPS (Secure HTTP access)**.
6. (Optional) If you selected **Local (Local Files or LAN)**, provide the **Windows account** username and **Password**for connecting to remote shares (not local folders).

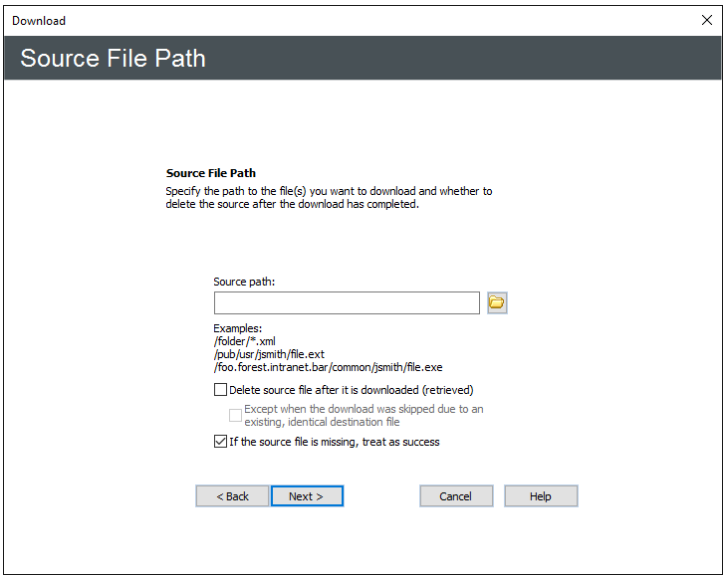
   These credentials are used only if/when a resource cannot be accessed using the credentials under which the EFT service is running. The **Optional credentials override** feature allows you to specify an alternate set of logon credentials for accessing remote network shares to which the EFT service account may not have access (due to security constraints).

   If alternate credentials are specified, EFT will use its current security token (associated with the “Log on as” account specified in the EFT service settings) for local folder access and then new security token (associated with the alternate logon credentials) for the remote source folder accessed over network connections (e.g. network shares).

   - Think of Local Transfer as an operation (offload or download) with a remote server.
   - Think of "Optional credentials override") as "credentials to access remote server."

- For download action, it is "credentials for source folder."
- For copy/move (offload), it is "credentials for destination folder."
- "Credentials to access local folder" ("source" for offload and "dest" for download) is Event Rule execution context (EFT account, or Folder Monitor account for FM rules, or Connected Client account for client-originated rules on an AD site):
  - Offload: local (EFT) => remote ("override credentials")
  - Download: local (EFT) <= remote ("override credentials")
  - TEST1: Offloads file from "local" Share A (access as EFT account, i.e., X) to "remote" folder B (access as Y) => Fails, as X has no permissions on A.
  - TEST2: Downloads file from "remote" Share A (access as Y) to "local" folder B (access as EFT account, i.e., X) => Succeeds, as Y has permissions on A and X has permissions on B.

7. If you chose anything but **Local**do the following; otherwise, skip to the Source File page step.
   a. In the **Host address**box, type the IP or host address of the EFT to which you want to connect.
   b. The **Port**number for the selected protocol changes automatically based on the offload method. Provide a different port number, if necessary.
   c. In the **Username**and **Password** boxes, type the username and password used to authenticate.
8. Select the **Use connected client's login credentials to authenticate** check box if you want to use the local system account to authenticate. The availability of this check box is controlled by the Persist username and password credentials for use in Event Rule context variablescheck box on the Site's **Security**tab.
9. If you chose **SFTP**, provide the client SFTP certificate information.
10. If you chose a protocol that uses SSL (FTPS or HTTPS), provide the client and remote server's SSL certificate information.
11. If you are connecting to a remote host through a SOCKS server, click **SOCKS** and provide the SOCKS connection information.
12. If you are connecting to a remote host through a proxy, click **Proxy**. Provide the proxy connection information.
13. To specify transfer options and time stamps, click **Advanced**. Specify the advanced transfer options, such as connection retry attempts and delay between retries.
14. To specify pre or post commands for connections to a mainframe computer, refer to Pre and Post Commands
15. Click **Next**. The **Source File Path** page appears.

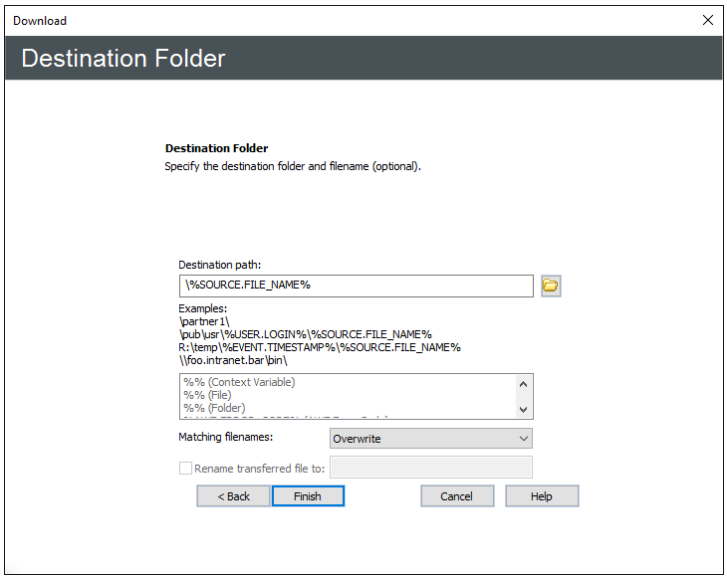


16. In the **Source path**box, provide the path to the file(s) that you want to download. For example, type:

    ```
    /pub/usr/jsmith/file.txt or
    \\mydomain\common\jsmith\file.txt
    ```

    If you type a path to a remote folder that does not exist, the Event Rule will fail.

17. Select the **Delete source file after it is downloaded** check box if you want to delete the file after it is retrieved. (If the file is marked read-only, it will not be deleted.)
    - Select the **Except when** ... check box if you do not want to delete the source file after it is downloaded if the download was skipped.
18. Select the **If source file is missing, treat as success check box** to treat remote file downloads as success, even if file is missing. (The client DLL in EFT doesn't have a mechanism for detecting if the file exists on the remote server or not.)
19. ***For LAN/local transfers only***, select the **If the source file is missing treat as success** check box if you want the Action to be considered successful even if the source file is missing.
20. Click **Next**. The **Destination File Folder**page appears.



21. The optional folder synchronization feature can also synch the destination folder with the source folder (2-way synchronization).
22. In the **Destination folder** box, click the folder icon and specify the location in which to save the downloaded file. You can insert variables by double-clicking them in the box below the **Destination folder** box.
    - In the **Matching filenames** box, specify whether to **Overwrite**, **Skip**, or **Numerate**files that exist with the same name. If **Overwrite**is selected, EFT performs a CRC match for the files.
23. If desired, select the **Rename transferred file to** check box, then specify a new name.
24. Click **Finish**, then click **Apply** to save the changes on EFT and/or add other Actions and Conditions to the Rule.

Protocol: Email Action

You can create an email notification Action for Event Rule and AS2 Transaction success/failure notifications. To save time, you can create an email notification template.

The EFT log will display an error message when a file larger than 30 MB is attached to a **Send notification email** Action in an Event Rule.

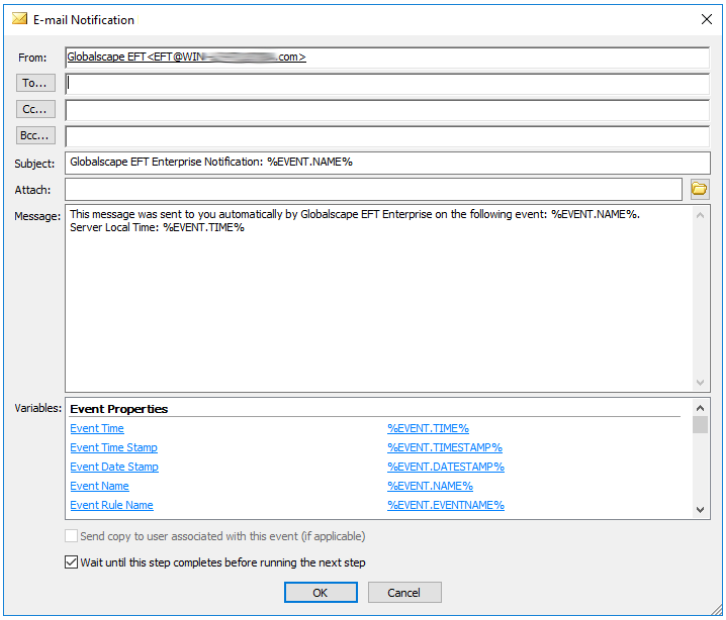
On Sites using AD Authentication, the EFT must have "Log On as a domain user" permission for email notifications to work.

To customize an Event Rule email message

1. Follow the procedure in Creating Event Rules to create a new Rule or select an existing Rule to which you want to add the Action.

   If you want to copy the involved user when the Event is triggered, the Rule must be based on a **User** Event.

2. In the **Actions**list, double-click **Send notification email** or click it, and then click **Add Action**.
3. Click the **[select]** link. The **email Notification Message** dialog box appears.



4. The **To** box displays the first email address defined in EFT address book on the **SMTP**tab, but you can change that, if needed. If you want to specify a different address than the prepopulated one from the **SMTP**tab, select the **Override 'From' field**check box, then specify the address.

5. Type the email address of other recipients in the **To**, **Cc**, and **Bcc**boxes or click **To**, **Cc**, or **Bcc** to open the **Select Names** dialog box, which is populated with names and email addresses defined on EFT in the **User Account Details** of each user account and on the SMTPtab. In the **Select Names** dialog box, you can type a name in the **Type Name or Select from List** box (not case sensitive) to find it in a heavily populated list. Select one or more recipients, and then click **To, CC**, or **BCC**. If you double-click a recipient, it is added to the **To**box. For multiple selections, press SHIFT (contiguous) or CTRL (non-contiguous). Click **OK** to save the changes.

   You can use the variable %USER.EMAIL%in the **To**, **Cc**, and **Bcc** boxes (%USER.EMAIL% is the email address of the logged-in user who is uploading a file, for example, if defined in the **User Account Details** dialog box).

6. In the **Subject**box, type a descriptive "title" for the email to indicate to the recipient the purpose of the email. You can also add variables. For example, if you want to see the reason an Event was triggered without opening the email, add the variable `%EVENT.REASON%`to the **Subject** line.

   For example, if you add the following text and variables to the Subject Line:

   ```
   EFT Notification: %EVENT.NAME%: %USER.LOGIN%,
   %EVENT.REASON%
   ```

   when username `jbite`uses the wrong password, an email is sent with the following **Subject** line:

   ```
   Globalscape EFT Notification:
           User Login Failed: jbite, Invalid password
   ```

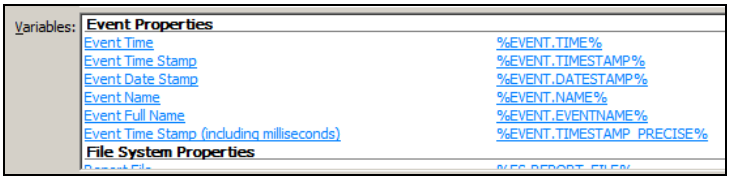
   %EVENT.NAME% is the Server-defined name for the Event (for example, File Renamed);
   %EVENT.EVENTNAME% is the user-defined name for the Event (for example, My File Renamed Event Rule).
   Also, be aware that your recipient might get hundreds of emails every day; therefore, "Here's the info you wanted" might not be descriptive enough.

7. In the **Attach**box, click the folder icon to browse for a file to attach to the email. You can use a specific file path or a context variable, that contains data.

%FS.REPORT_FILE% - The full path of the report generated by the Generate Report Action, including the file name. This variable can be used in copy/move, OpenPGP, and custom commands that have a failure Event defined, but should not be used for custom command actions that do not have a failure Event defined. In some cases, it may be more appropriate to use %FS.REPORT_CONTENT% because this variable represents a copy of the contents of the file rather than a link to the file, which is only good so long as the file exists. For example, since the file will be deleted when EFT stops processing the Event Rule, do not use this variable in email notifications; use %FS.REPORT_CONTENT% instead.

%FS.REPORT_CONTENT% - Contents of the report generated by the Generate Report Action. This variable is typically used after creation of an HTML report, in an email notification action, where it is desirable to embed the HTML contents of the report as the email body.

8. In the **Message**box, type the text of the email. You can use HTML tags within the body of the email. (Be sure to include the opening and closing <html> and <body> tags.) You can also define an email template for common emails and provide a link to the template in the **Message** area. If the account to which the email is sent accepts HTML-formatted email, you can format the email to suit your needs; you are only limited by your knowledge of HTML. (If the recipient's email server does not accept HTML email, the recipient will see the email in plain text.)
9. In the Variables box, click a property that you want to insert in the email message. The text surrounded by percent signs, the *context variable*, is inserted into the body of the email, and will be replaced by EFT with specific information about the Event when the email is sent. Review the available Variableswhen deciding which variables to add, because ***some variables cannot be used in email notifications***.



   - If you want only the information contained to the variable in your email message, click the context variable in the right column of the **Variables** box. (For example, if you select `%EVENT.TIME%` in the right column, the time will be displayed without a text label.)
   - If you want the information and a label, click the text in the left column of the **Variables**box. (For example, if you click Event Time, the label and the time appear in the email.)
10. If this is a User Event and you want to send a copy of the message to the involved user, select the **Send copy to user** check box.

11. (Optional) The **Wait until this step completes before running the next step** check box is selected by default. When the check box is selected, you can select the "If failed" action, and populate it with actions to run in case the rule fails. **To allow the next step to run before this action completes**, clear the check box. If check box is not selected, a prompt appears to confirm: "This step will be executed asynchronously (non-blocking), which means EFT won't wait for this step to be completed before running the next step. This could yield undesirable results if the next step depends on the output or outcome of this one. Are you sure you want to make this action asynchronous?" (All actions in the IF FAILED section are lost if the parent action is switched from async to sync mode.)
12. Click **OK**.
13. Click **Apply**. When the Event is triggered, the email notification is sent. The **Send notification email** Action in Event Rules puts the message into a send queue unless "Stop processing this rule" is enabled for a failed Action.

Related Topics

- Creating an email Notification Template
- Adding an Action to an Event Rule
- Variables

Creating an Email Notification Template

The Conditions and Actions for every Event Rule you create, including email notifications, is saved in EFT's configuration file. Each time the administration interface connects, it reads in the configuration file. Multiple Event Rules and email notifications can grow the configuration file quite large. If you expect to have numerous email notifications that are basically the same (for example, you have default text that you always want to appear in the body of the email), you can define the body of the email in an HTML file, then reference it in the **Message**box of the **Email Notification Message**.

To create an email notification template

1. Create an HTML document that contains the text that will be the body of the email notification. You can include any HTML tags and EFT variables. For example:

```
<HTML>
   <BODY>
        <P>This message was sent to you automatically by
Globalscape
        EFT on the following event: %EVENT.NAME%.</p>
        <HR>
        <P><B>Server Local Time:</B> %EVENT.TIME%</P>
        <P><B>Logon Name:</B> %USER.LOGIN%</P>
        <P><B>Email Address:</B> %USER.EMAIL%</P>
        <P><B>Home Folder:</B> %USER.HOME_FOLDER%</P>
   </BODY>
</HTML>
```

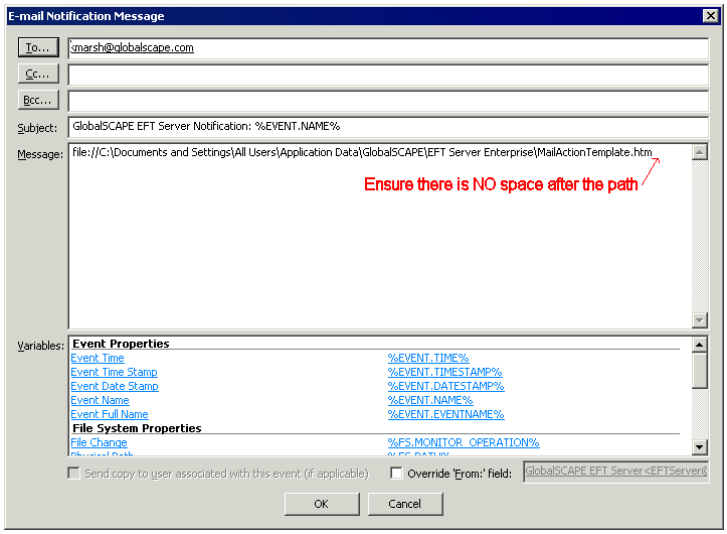
2. Define the email adding each of the variables that you want. You can add your custom EFT administrator signature, your company's logo, any information that you need to pass on to the user, and so on. Be sure to include the opening and closing <html> and <body> tags. Use the interface to add variables and labels to the message.
3. Copy and paste the message into a text file, and save it with an **.htm** extension.

   Review your tags carefully, however, since no HTML-code verification is performed. As a test, you can copy and paste the text into Notepad, save it with an .htm extension, and then open it in your browser.
4. Save the file in a location that can be accessed by EFT. (If you are logging into EFT on an Active Directory-authenticated Site, the Event Rule engine is running as that logged-in user, so the user account must have access to the template.)
5. Define the Event Rule and add the email notification.

6. In the **Message**box of the **email Notification Message**dialog box, type `file://`and the path to the email template, and then click **OK**. For example, type:

   ```
   file://C:\Documents and Settings\All Users\Application Data\Globalscape\EFT Server\MailActionTemplate.htm
   ```

   IMPORTANT: There can be no spaces or line breaks before or after the link!



7. Click **OK** to add the notification to the Event Rule.

The referenced HTML file will appear in the body of the email that is triggered by EFT. It is highly recommended that you do a test to be sure you get the results you want.

Send an Email Notification When a Certain User Uploads a File

Refer to the Globalscape Knowledgebase topic #11151 for information about sending an email notification when a certain user uploads a file.

Protocol: Synchronize Action

(Requires FTC module) The **Protocol: Synchronize Action** allows you to make a local folder list match a remote folder, or a remote folder match a local folder. The Synchronize Action is available for any Event Rule for which copy, move, or download actions are used. The wizard allows you to synchronize or mirror the folders:

With respect to EFT rules:

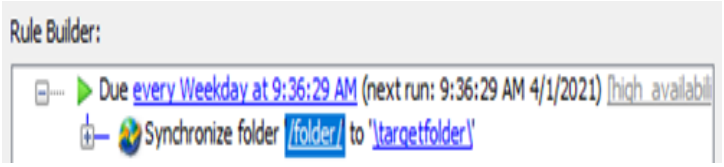
- "Mirror local – duplicate EFT's contents to the remote server"
- "Mirror remote – duplicate the remote server's contents to EFT"

With respect to RAM Agent rules

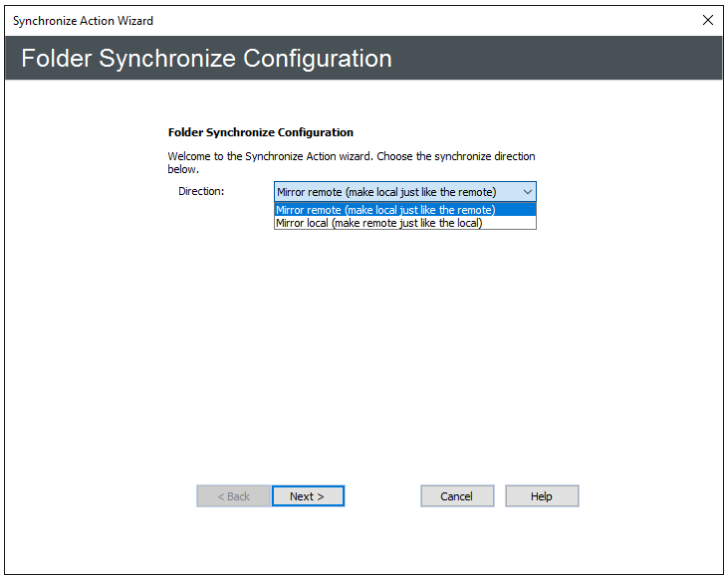
- "Mirror local – duplicate Agent's contents to the remote server"
- "Mirror remote – duplicate the remote server's contents to the Agent"

To define the Synchronize Action

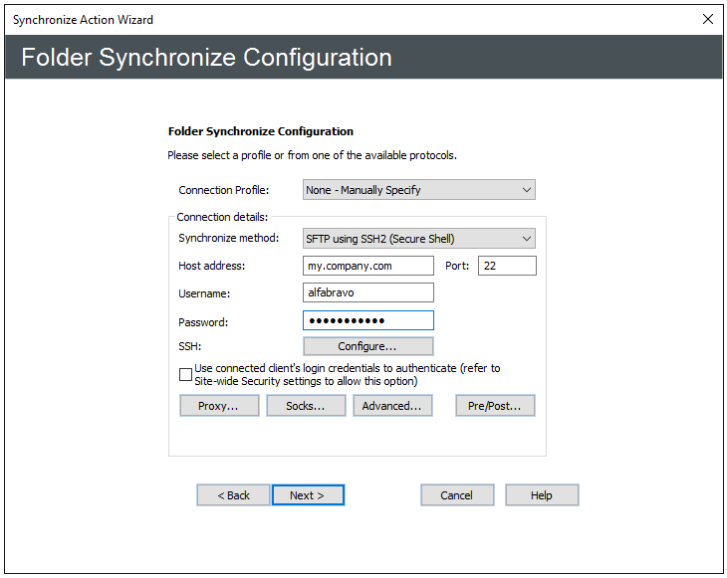
1. Follow the procedure in Creating Event Rules or select the Rule to which you want to add the Action.
2. In the **Actions**list, click **Protocol: Synchronize**. The Rule parameters are added to the Rule in the **Rule Builder**.



3. Click one of the undefined parameters where the parameters are listed in the **Rule Builder**. The **Synchronize Action** wizard appears.

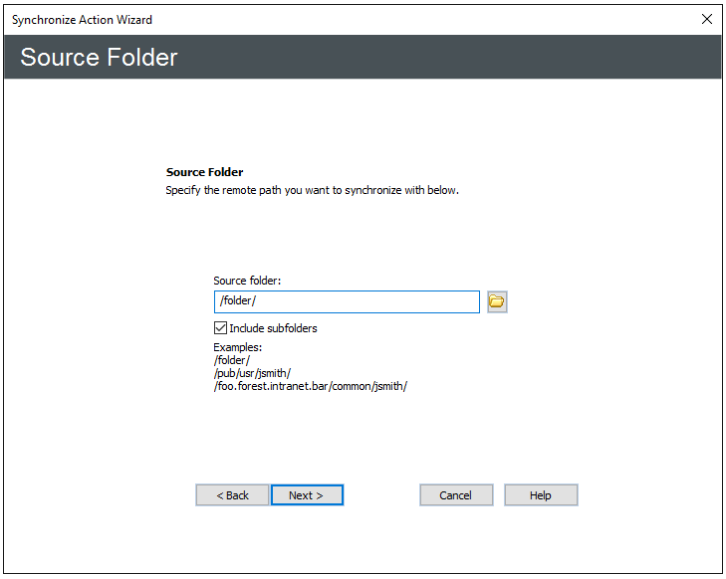


4. In the **Direction**list, specify whether to **Mirror remote**or **Mirror local,** then click **Next**. The **Configuration**page appears.



5. In the **Connection Profile** box, specify a connection profile for this Event. If none is specified, you will need to configure the **Connection details** as described below.
6. Click the **Synchronize method** list to specify a **method**for the connection: **FTP (standard File Transfer Protocol)**, **FTP SSL/TLS (AUTH TLS)**, **FTP with SSL (Explicit encryption)**, **FTP with SSL (Implicit encryption)**, **SFTP using SSH2 (Secure Shell)**.
7. In the **Host address**box, type the IP or host address of the EFT to which you want to connect.

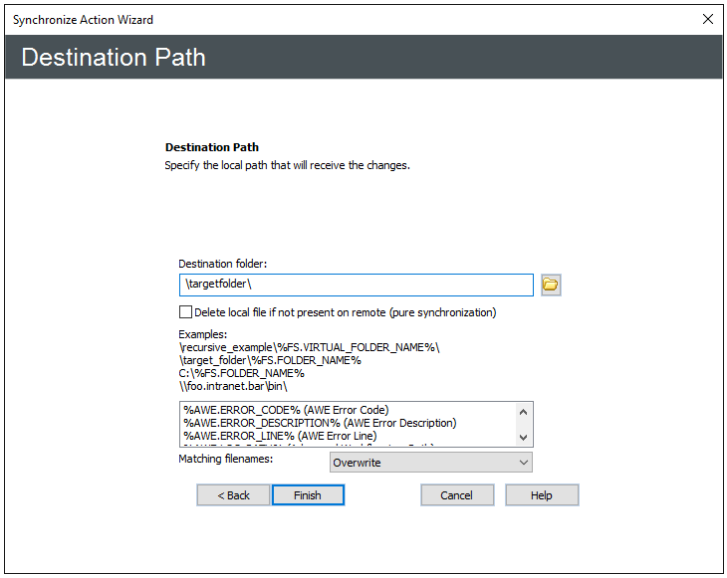
8. The **Port** number for the selected protocol changes automatically based on the offload method. Provide a different port number, if necessary.
9. In the **Username**and **Password** boxes, type the username and password used to authenticate.
10. Select the **Use connected client's login credentials to authenticate** check box if you want to use the local system account to authenticate. The availability of this check box is controlled by the Persist username and password credentials for use in Event Rule context variablescheck box on the Site's **Security**tab.
11. If you chose **SFTP**, provide the client SFTP certificate information.
12. If you chose a protocol that uses SSL (FTPS or HTTPS), provide the client and remote server's SSL certificate information.
13. If you are connecting to a remote host through a SOCKS server, click **SOCKS** and provide the SOCKS connection information.
14. If you are connecting to a remote host through a proxy, click **Proxy**. Provide the proxy connection information.
15. To specify transfer options and time stamps, in the Offload wizard, click **Advanced**. Specify the advanced transfer options, such as connection retry attempts and delay between retries.
16. Click **Next**. The **Source Folder** page appears.



17. In the **Source path**box, provide the path to the file(s) that you want to synchronize. For example, type:

```
/pub/usr/jsmith/file.txt or
\\mydomain\common\jsmith\file.txt
```

18. Select the **Include subfolders** check box if you also want to synchronize the subfolders of the source folder.
19. Click **Next**. The **Destination Path** page appears.



20. In the **Destination folder** box, click the folder icon and specify the location in which to save the downloaded file. You can insert variables by double-clicking them in the box below the **Destination folder** box. If you type a path to a remote folder that does not exist, the Event Rule will fail.
21. To make local folder match the remote folder, select the **Delete local file if not present on remote**.
22. In the **Matching filenames** box, specify whether to **Overwrite**, **Skip**, **Skip if size is the same**, **Skip if size and time are the same**, **Smart Overwrite**, or **Numerate** files that exist with the same name. (Refer to Smart Overwrite for more information about Smart Overwrite.) This setting only applies to the initial transfer, not when the transfer is interrupted and then resumed. When resuming, EFT will follow the Smart Overwrite settings (that is, performs a CRC match for the files; if the files are identical, the destination file is not overwritten).
    - **Overwrite**—Overwrite any existing file with the same name.
    - **Skip**—Skip the transfer if a file with the same name exists in the destination directory.
    - **Skip if size is the same**—Skip the transfer if a file with the same name and size exists in the destination directory.
    - **Skip if size and time are the same**—Skip the transfer if a file with the same name, size and timestamp exists in the destination directory. *When using this overwrite method, the preserve remote/local time

stamps option must be enabled or the files may always be overwritten. These settings can be found under the Advanced Options of the connection profile.

- **Smart Overwrite**—EFT performs a CRC match for the files. If the files are identical, the destination file is not overwritten. Refer to Smart Overwrite for more information about this feature. (Supported only on FTP transfers.)
- **Numerate**—If a file in the destination folder has the same name as the file you are transferring, EFT renames the transferred file to "Copy of file.txt." If the same transfer occurs again, EFT renames the transferred file to "Copy (2) of file.txt" and so on.

23. Click **Finish**, then click **Apply** to save the changes on EFT and/or add other Actions and Conditions to the Rule.

> **NOTE:** If **Skip if size and time are the same** is selected, EFT will skip overwriting when the filename, size and time stamp of the files are identical. When using this overwrite method, the preserve remote/local time stamps option must be enabled or the files can always be overwritten. These can be found in the **Advanced** options under the **Connection Details** area on the configuration page of the wizard.
>
> Synchronization action fails to delete file with **Numerate**set.

Protocol: Upload Action

(Requires FTC module) You can configure EFT to upload (also known as "offload") files to a specific location using a particular protocol whenever certain Events occur, such as when a report is created. You must provide EFT with connection information (protocol and login details) and file information (source path and destination path).

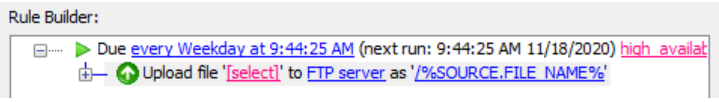
The Upload Action can be applied to all File Server Events; the User Events "User Quota Exceeded," "User Logged In," and "User Logged Out"; and the Server Events "Timer" and "Log Rotated."

- If you create an Upload Rule that sends a file transfer activity report, the file transfer that triggered the Rule is not included in the report.
- When you add a Upload file to host action to a rule, the Client FTP offload engine performs retries upon failures (network failures is the typical example) based upon the settings in the Advanced Options dialog box. Be aware that the **Protocol Upload** Action does the transfer, including all retries, before moving on to the next Action, such as an email notification. A long-running transfer that also retries numerous times with large delays will cause the Event Rule to take a long time to complete.
- A **Move** Action over the local file system updates the variables `FS.PATH`, `FS.FILE_NAME`, and `FS.FOLDER_NAME`to match the NEW file location.
- When EFT opens a file for copy, it uses FILE_SHARE_READ sharing mode. This mode ensures that a file cannot be changed by another process while EFT copies it, preventing corruption of the file.
- Configure the retry logic in the Copy Action for **Local (Local Files or LAN)** offload events. If an Event Rule triggers and you had large amounts of small files that were copied over a LAN share, some of the files could copy over at 0 KB. This retry logic will try the copy again if the file is locked or in use so the destination file will not have a 0 kb size.

Refer to Connection Profiles for details of setting up a Connection Profile before defining the Action.

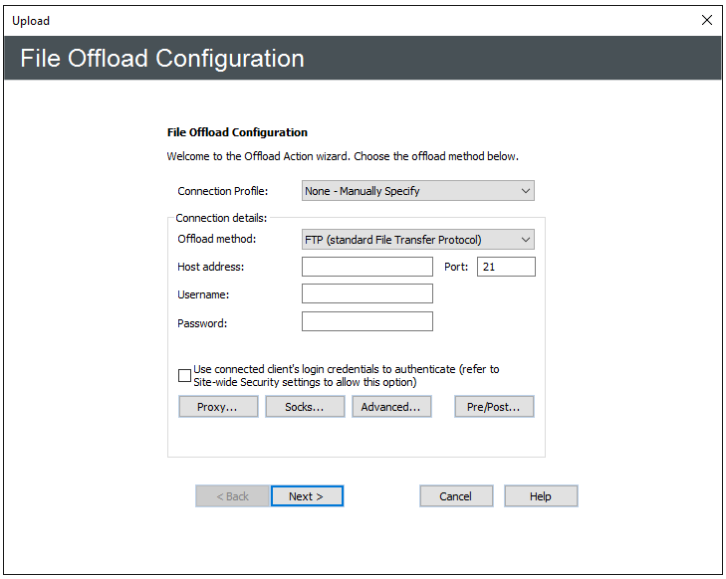
To configure EFT to upload files

1. Follow the procedure in Creating Event Rules, or select the Rule to which you want to add the Action. For example, create a Scheduler (Timer) Event.
2. In the right pane, in the **Actions**list, double-click **Protocol: Upload Action**.



3. In the **Rule Builder**, click one of the undefined parameters (for example, '[select]' or '/%SOURCE.FILE_NAME%').

   The **Upload/File Offload Configuration** wizard appears.



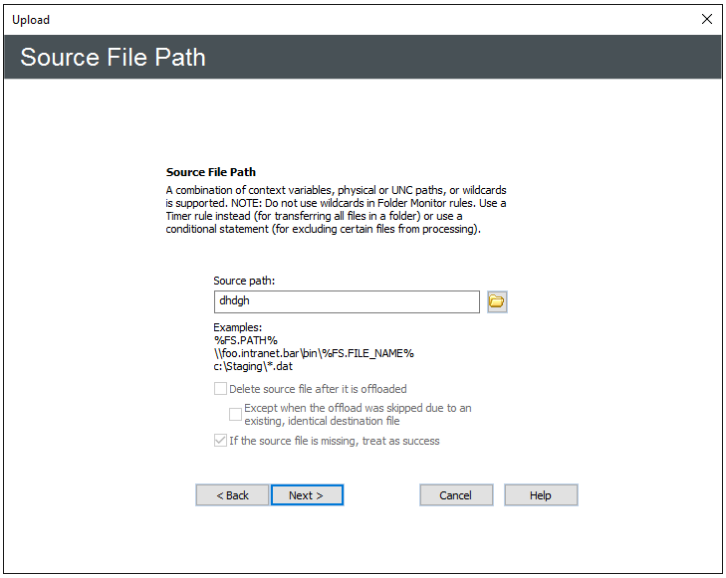
4. In the **Connection Profile** box, specify a connection profile for this Event. If none is specified, you will need to configure the **Connection details** as described below.
5. On the **Offload method**box, specify a protocol type for the connection: **Local (Local File or LAN)**, **FTP (standard File Transfer Protocol)**, **FTP SSL/TLS (AUTH TLS)**, **FTP with SSL (Explicit encryption)**, **FTP with SSL (Implicit encryption)**, **SFTP using SSH2 (Secure Shell)**, **HTTP (HyperText Transfer Protocol)**, **HTTPS (Secure HTTP access)**.
6. (Optional) If you selected **Local (Local Files or LAN)**, under **Optional credentials override**, provide the **Windows account**username and **Password** for connecting to remote shares (not local folders).
   - These credentials are used for the remote ***destination***folder ONLY for upload actions. The source (Local) folder will still use EFT server service account at all times. (When using download (PULL) actionsover LAN, the same concept applies, but credentials will be used for the source directory and EFT server service account for the destination.)
   - Only if/when a resource cannot be accessed using the credentials under which the EFT service is running do you need to include the **optional credentials.**The **Optional credentials override** feature allows you to specify an alternate set of logon credentials for accessing the ***destination*** network shares to which the EFT service account may not have access

(due to security constraints).

- If alternate credentials are specified, EFT will use its current security token (associated with the "Log on as" account specified in the EFT server service settings) for LOCAL folder access and then a new security token (associated with the alternate logon credentials) for the remote ***destination*** folder accessed over network connections (e.g. network shares).
- Think of Local Transfer as an operation (offload or download) with a remote server.
- Think of "Optional credentials override" as "credentials to access remote server."
- For download action, it is "credentials for source folder."
- For upload (offload), it is "credentials for destination folder."
- "Credentials to access local folder" ("source" for offload and "dest" for download) is Event Rule execution context (EFT account, or Folder Monitor account for FM rules, or Connected Client account for client-originated rules on an AD site):
  - Offload: local (EFT) => remote ("override credentials")
  - Download: local (EFT) <= remote ("override credentials")
  - TEST1: Offloads file from "local" Share A (access as EFT account, i.e., X) to "remote" folder B (access as Y) => Fails, as X has no permissions on A.
  - TEST2: Downloads file from "remote" Share A (access as Y) to "local" folder B (access as EFT account, i.e., X) => Succeeds, as Y has permissions on A and X has permissions on B.

7. If you chose **Local**, click **Advanced** to configure retry attempts, then skip to the Source File Path pagestep.
8. If you chose anything but **Local**do the following;
   a. In the **Host address**box, type the IP address.
   b. The **Port**number for the selected protocol changes automatically based on the offload method. Provide a different port number, if necessary.
   c. (Optional) Provide the **Username**and **Password** needed to establish the connection.
   d. To configure advanced options, click **Advanced**. Refer to Advanced Transfer Options for details.
9. Select the **Use connected client's login credentials to authenticate** check box if you want to use the local system account to authenticate. The availability of this check box is controlled on the Site's **Security**tab by the Persist username and password credentials for use in Event Rule context variablescheck box.

10. If you chose **SFTP**, provide the client SFTP certificate information.
11. If you chose a protocol that uses SSL (FTPS or HTTPS), provide the client and remote server's SSL certificate information.
12. If you are connecting to a remote host through a SOCKS server, click **SOCKS** and provide the SOCKS connection information.
13. If you are connecting to a remote host through a proxy, click **Proxy**. Provide the proxy connection information.
14. To specify transfer options and time stamps, in the Offload wizard, click **Advanced**.Specify the advanced transfer options.
15. (optional) To define commands to occur before and after this operation, click **Pre/Post**. Refer to Pre and Post Commands for details.
16. Click **Next**. The **Source File Path** page appears.



17. In the **Source path**box, provide the path to the file(s) that you want to offload. (No validation is performed.) For example, type:

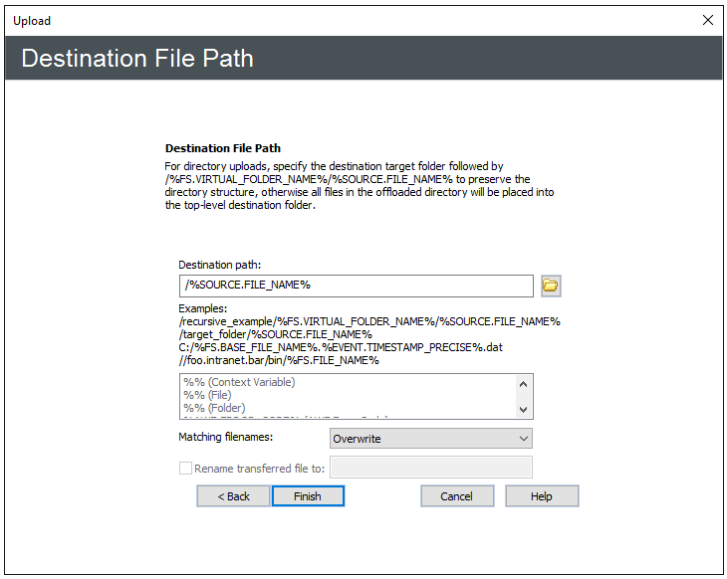
    `C:\Staging\*.dat or \\mydomain\common\jsmith\file.txt`

    You can leave **Source path** blank or use %FS.PATH% to offload the files associated with the Event that triggered the Action. In a Timer Event, there is no context variable available for the path, so you must specify a file name.

18. Select the **Delete source file after it has been offloaded** check box if you want to delete the file after it is copied/moved. (If the file is marked read-only, it will not be deleted.)

- Select the **Except when**check box if you do not want to delete the source file after it is offloaded if the offload was skipped.

19. Select the **If the source file is missing treat as success** check box if you want the Action to be considered successful even if the source file is missing.
20. Click **Next**. The **Destination File Path**page appears.



21. In the **Destination path** box, specify the location in which to save the offloaded file. (No validation is performed when you type a path; the Folder icon is only available for local transfers.)

    If you type a path to a folder that does not exist, the Event Rule will fail. Be sure you have the path defined correctly, e.g., make sure to use the proper slash. In general, forward slashes / are used in remote paths, and backward slashes \ are used in local Windows paths. Do not use both.

    - You can specify variables, such as `\pub\usr\%USER.LOGIN%\%FS.FILE.NAME%`.
    - In the **Variables**box, double-click the variable(s) that you want to add to the path.
    - In *Move*Actions over the LOCAL FILE SYSTEM, the %FS.PATH%, %FS.FILE_NAME%, and %FS.FOLDER_NAME% context variables are updated to match the new file location.
    - In the **Matching filenames** box, specify whether to **Overwrite**, **Skip**, **Smart Overwrite**, or **Numerate**files that exist with the same name. (Refer to Smart Overwrite for more information about Smart Overwrite.) This setting only applies to the initial transfer, not when the transfer is interrupted and then resumed. When resuming, EFT will follow the Smart

Overwrite settings (that is, performs a CRC match for the files; if the files are identical, the destination file is not overwritten).

- **Overwrite**—Overwrite any existing file with the same name.
- **Skip**—Skip the offload if a file with the same name exists in the destination directory.
- **Smart Overwrite**—EFT performs a CRC match for the files. If the files are identical, the destination file is not overwritten. Refer to Smart Overwrite for more information about this feature. (Supported only on FTP transfers.)
- **Numerate**—If a file in the destination folder has the same name as the file you are transferring, EFT renames the transferred file to "Copy of file.txt." If the same transfer occurs again, EFT renames the transferred file to "Copy (2) of file.txt" and so on.

- If you want to rename the file, select the **Rename transferred file to** box and specify a new name.
  - You can rename the file when it is transferred. For example, when "myfile.doc" is uploaded, you might want to save it as "status_%EVENT.DATESTAMP%.doc" or something else more identifiable.
  - You can also use variables in the **Rename transferred file to** box. For example, /%FS.FILE_NAME%.%EVENT.TIMESTAMP%
  - For LAN renames, you must include the full path to the file.
  - Only FTP and FTPS are currently supported.
  - EFT executes a RNFR + RNTO sequence for FTP transfers on the remote server. If the remote server supports cross-folder rename (as EFT does), it is possible for Rename-Pathname-Filename variable to point to a different folder than the Offload Destination folder.
  - The Offload transaction status will be FAILED if the rename fails, even though the file was transferred.
  - The **Status Viewer** will display the Rename-To value in the **Remote Path** field for Offload.

22. Click **Finish**then click **Apply** to save the changes on EFT and/or add other Actions and Conditions to the Rule.

    If you are copying or moving the file to another location, and the file upload is a regularly occurring Event with a file of the same name, in the **Offload Action** wizard, add the variables `%EVENT.DATESTAMP%`and/or `%EVENT.TIMESTAMP%` to the path so that the date (YYYYMMDD) and/or time (HHMMSS) are added to the filename when it is moved/copied. Do ***not***use `%EVENT.TIME%`, because the colon (for example, `28 Aug 07 10:01:56`) makes it unsuitable for file naming.

For example, in the **Offload Action wizard**, in the **Destination path** box, provide the path and variables. For example, type:

```
C:\Documents and Settings\administrator\My
Documents\upload\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%_%FS.F
ILE_NAME%
```

With this path and variables, when a file is uploaded to the monitored folder, the file is moved to \My Documents\upload and the date and time are prepended to the filename. For example, 20080422_101212_ mydailyprogress.doc.

Related Topics

- Using Wildcards with Event Rule Actions
- Copying or Moving a File Triggered on Monitor Folder Event and Renamed

Adding a Workflow Action to an Event Rule

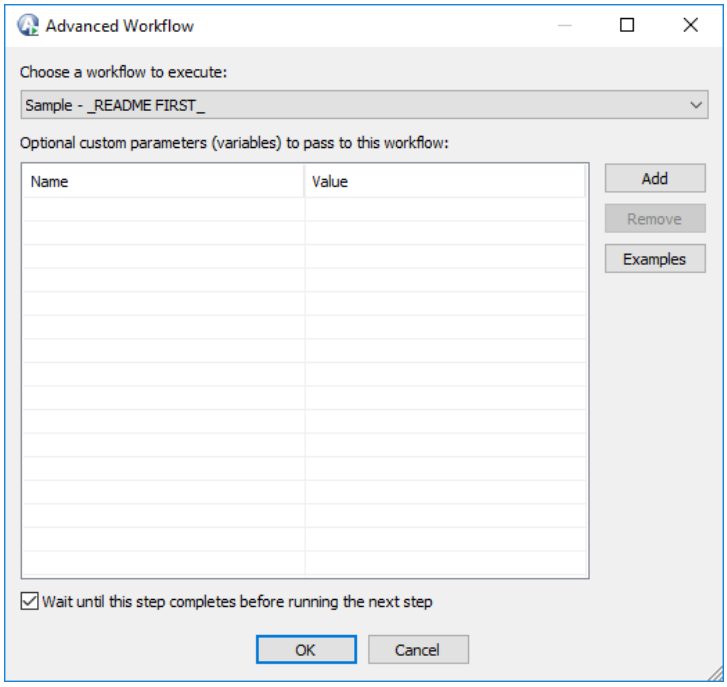
(Requires the Advanced Workflow module.) With Advanced Workflow Actions, EFT does not wait for a reply before returning control to the Event Rule thread, *unless* an "if failed" Action was specified, such as **Stop Processing this Rule**, in which case the Action waits for a return message indicating success or failure from the invoked process.

The workflows created for use in Event Rules are executed using the EFT server administrator credentials, unless you specify otherwise. If a resource cannot be accessed using the credentials under which the EFT service is running, you need to include the **optional credentials for the destination server.**

- Think of "Local Transfer" as an operation (offload or download) with a remote server.
- Think of "Optional credentials override" as "credentials to access remote server."
    - For download action, it is "credentials for source folder."
    - For copy/move (offload), it is "credentials for destination folder."
- "Credentials to access local folder" ("source" for offload and "dest" for download) is Event Rule execution context (EFT account, or Folder Monitor account for FM rules, or Connected Client account for client-originated rules on an AD site):
    - Offload: local (EFT) => remote ("override credentials")
    - Download: local (EFT) <= remote ("override credentials")
    - TEST1: Offloads file from "local" Share A (access as EFT account, i.e., X) to "remote" folder B (access as Y) => Fails, as X has no permissions on A.
    - TEST2: Downloads file from "remote" Share A (access as Y) to "local" folder B (access as EFT account, i.e., X) => Succeeds, as Y has permissions on A and X has permissions on B.

To add a Workflow to an Event Rule

1. Create a Workflow.
2. Create an Event Rule.
3. In the **Actions**list, double-click **Script: Advanced Workflow**. The Action is added to the Rule.
4. In the **Rule Builder**, click the **Advanced Workflow** link. The **Advanced Workflow** dialog box appears.



5. The defined Workflows appear in alphabetical order in the **Choose a workflow to execute**list (at the top of the **Advanced Workflow** dialog box). Click the down arrow to select a Workflow.
6. (Optional) Specify custom parameters to pass to the Workflow in the **Name** and **Value** columns, and then click **Add**.
7. (Optional) The **Wait until this step completes before running the next step** check box is selected by default.
    a. When the check box is selected, you can select the "If failed" action, and populate it with actions to run in case the rule fails.
    b. To allow the next step to run before this action completes, clear the check box. If check box is not selected, a prompt appears to confirm: "This step will be executed asynchronously (non-blocking), which means EFT won't wait for this step to be completed before running the next step. This could yield undesirable results if the next step depends on the output or

outcome of this one. Are you sure you want to make this action asynchronous?" (All actions in the IF FAILED section are lost if the parent action is switched from async to sync mode.)

8. Click **OK**. The **Advanced Workflow** link in the **Rule Builder** updates with the name of the Workflow.
9. Add other Actions as needed, and then click **Apply** to save the changes on EFT.

Script: Custom Command Action

(Requires EAM) The topics below provide the procedures for configuring and using Commands in EFT.

- Introduction to Commands
- Creating a Command with the Custom Command Wizard
- Editing a Command
- Custom Command Example
- Viewing and Deleting Commands
- Enabling and Disabling Commands
- Script: Custom Command Action
- Command Permissions

Custom Commands

EFT's *Custom Commands*can execute programs, scripts, or batch files with or without command line arguments, providing administrators almost limitless extensibility. These Commands can be invoked directly by a user from their client (if permitted by the Server administrator) or as an automated Action from EFT's Event Rules.

When the Event Rule is triggered, EFT executes the specified custom Command and attributes. To configure EFT to execute Commands, you first create the command, then add the command to an Event Rule. In the administration interface, the Commands appear in the tree in the left pane within the Site for which they are defined.

With the **Server** tab selected, when you click the **Commands** node on the **Server** tab, the **Commands List** appears in the right pane.

- Click **New**to open the **Custom Command Wizard**and create a new Command.
- Click a Command then click **Edit**to edit an existing Command.
- Select a Command in the list, and then click **Remove** to delete it. (A confirmation message appears.)

Related Topics

- The Custom Command Wizard
- Editing a Command
- Viewing and Removing Commands
- Enabling and Disabling Commands
- Custom Command Example
- Script: Custom Command Action

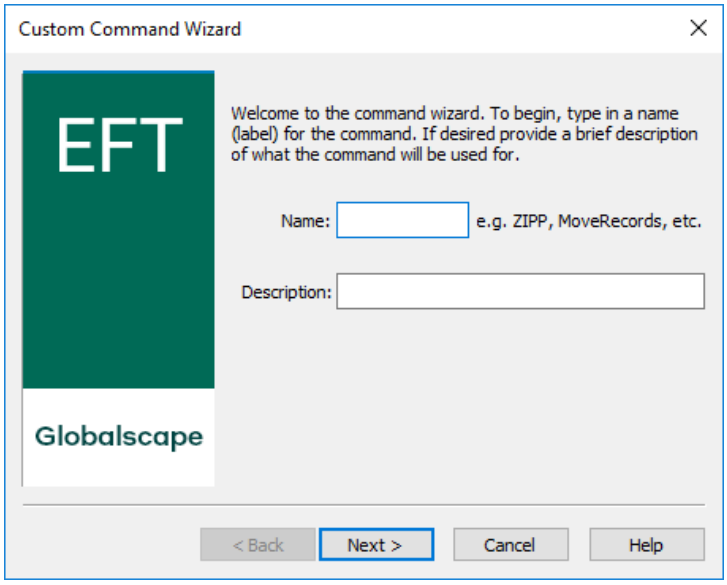
Creating a Command with the Custom Command Wizard

The **Custom Command** wizard steps you through the process of creating a Command to tell EFT to execute programs, scripts, or batch files.

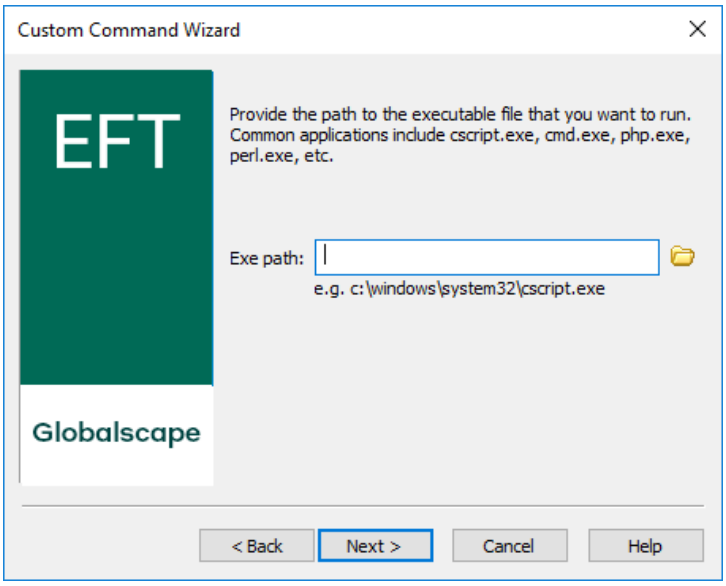
To create a command with the Custom Command wizard

1. In the left pane, right-click the **Commands**node, and then click **New Command**.
2. Click the **Commands**node in the left pane, then, in the right pane, click **New**.
3. Press CTRL+M.

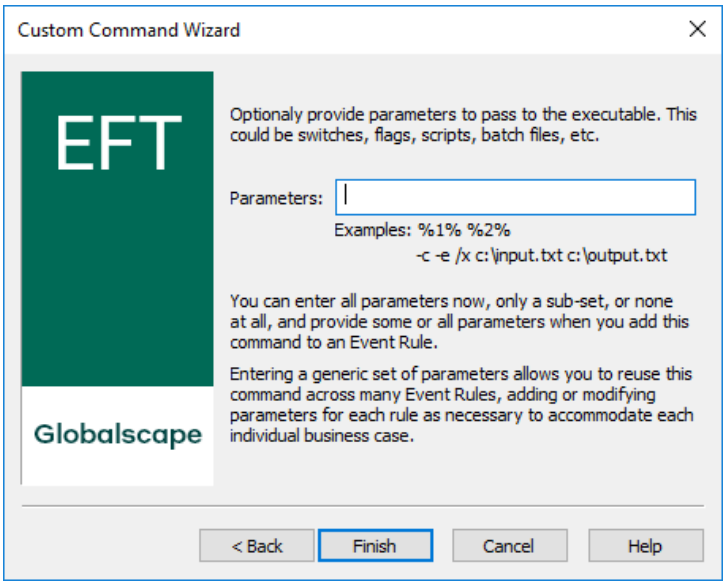
   The **Custom Command Wizard**appears.



4. In the **Name**box, type a descriptive name for the command. You will reference the Command name in Event Rules, so you should give the Command an intuitive name. For example, instead of `Command 1`, you might call it `Run CScript`.
5. Provide a **Description**that will help you identify the command.
6. Click **Next**. The path page appears.

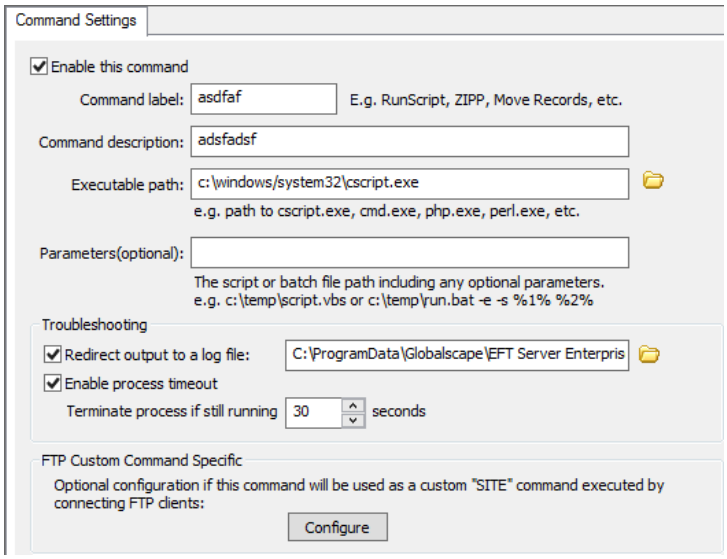


7. In the **Path to executable**box, browse to or type the path to the executable. For example, you can specify a program, a batch file, or a Windows scripting executable, such as cscript.exe or wscript.exe. If you are connected to EFT remotely, you can type the path to the file, but be sure the path is relevant to the EFT computer, not the remote interface.

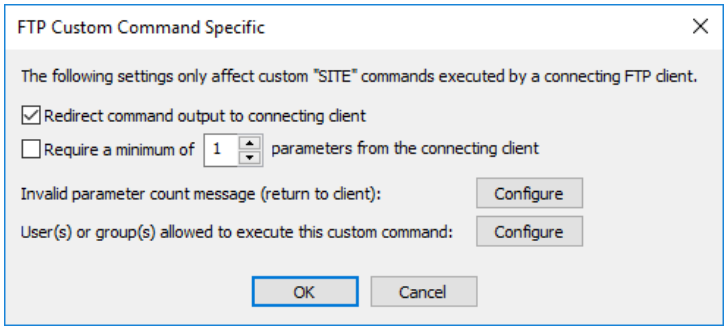


8. (Optional) Specify any required parameters. Alternately, you can specify the parameters when you add the Command to an Event Rule. If there are "standard" parameters that you will always use with the script, you can specify them here, then modify them or add additional parameters when you add the Command to an Event Rule.

9. Click **Finish**. The Command is added to the **Commands**node for the Site and appears in the **Command Settings** tab in the right pane.



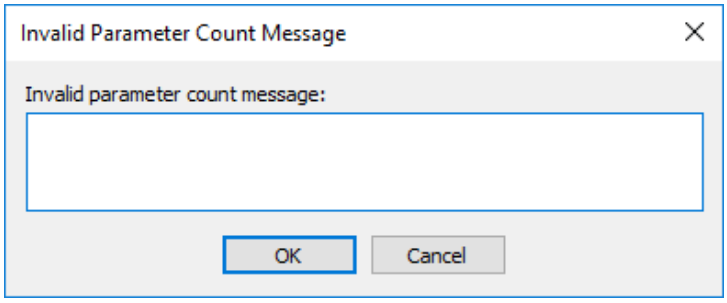
10. If the Command is a custom SITE command executed by a connecting FTP client, you can also configure the **FTP Custom Command Specific** settings, the invalid parameter count message, and which Groups are allowed to execute the Command by clicking **Configure**. The **FTP Custom Command Specific** dialog box appears.



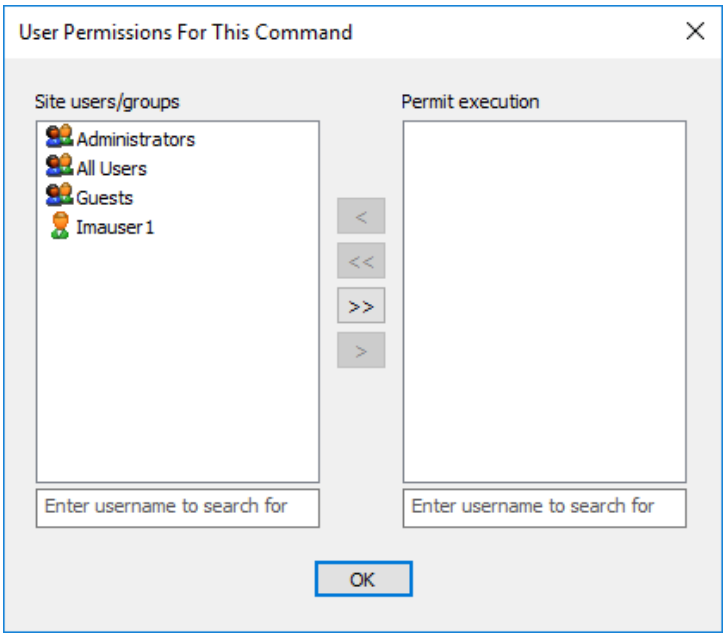
11. Select the **Redirect command output to connecting client** check box to redirect the output from the executed command to the client in a 220 response message. If the check box is not selected, then the output of the command is not returned to the client, even though the command is still executed on the server.

Redirecting command output can help the end user ascertain whether the command worked properly (depending on result codes returned by the script or application executed by the custom command on the server).

12. If you want to force the FTP client to send a minimum number of parameters, select the **Require a minimum of** check box and specify the minimum number of parameters required.
    - To provide a message that users will receive when the parameter number is not met, next to **Invalid parameter count message**, click **Configure**. Provide the message, and then click **OK**.



    - To specify the users and Groups that can execute the Command, next to **User(s) or group(s) allowed to execute this custom command**, click **Configure**. Double-click the users and/or groups, or use the arrows to move them between the **Site users/groups**list and the **Permit execution** list. To search for specific users, type the username in the search box.



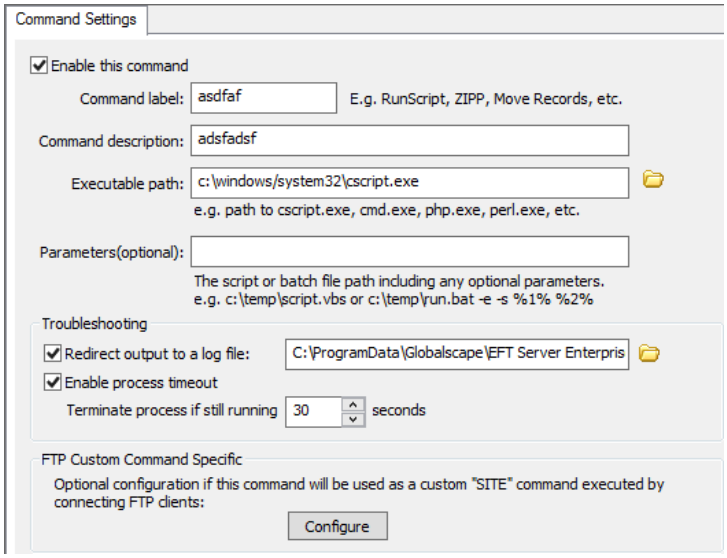
13. Click **OK**, then click **Apply** to save the changes on EFT.

Editing a Command

The procedure below describes how to edit a command that you can execute with an Event Rule. For a general introduction to Commands, refer to Introduction to Commands. To create a command, refer to Creating a Command with the Custom Command Wizard.

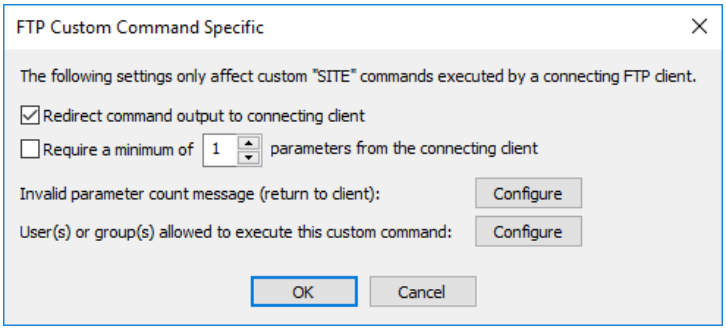
To edit a command

1. In the administration interface, connect to EFT, then click the **Server**tab.
2. On the **Server**tab, expand the Site node for the Site that you want to configure, and then click the **Commands**node.
3. In the right pane, double-click the Command that you want to edit. The **Command Settings**tab appears.

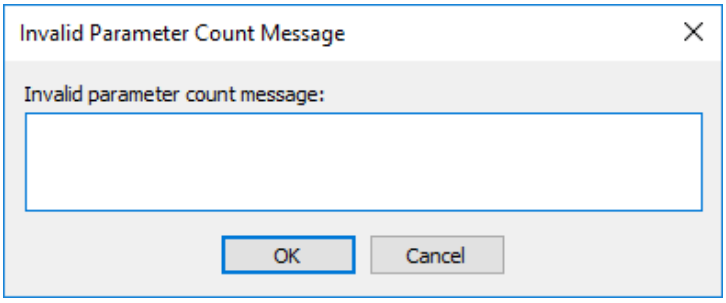


4. The **Command label**box displays the name you gave the Command. You will reference the Command label in the Event Rule and **Custom Command** dialog box (in the **Select Command** drop-down menu), so you should give the Command an intuitive name. For example, instead of `Command 1`, you might call it `Run CScript`.
5. The **Command description**box displays the description that you gave the Command.
6. The **Executable path**box displays the path to the file that you want the Command to execute.
7. The **Parameters**box displays any parameters that the client must send. (Parameters are optional.)

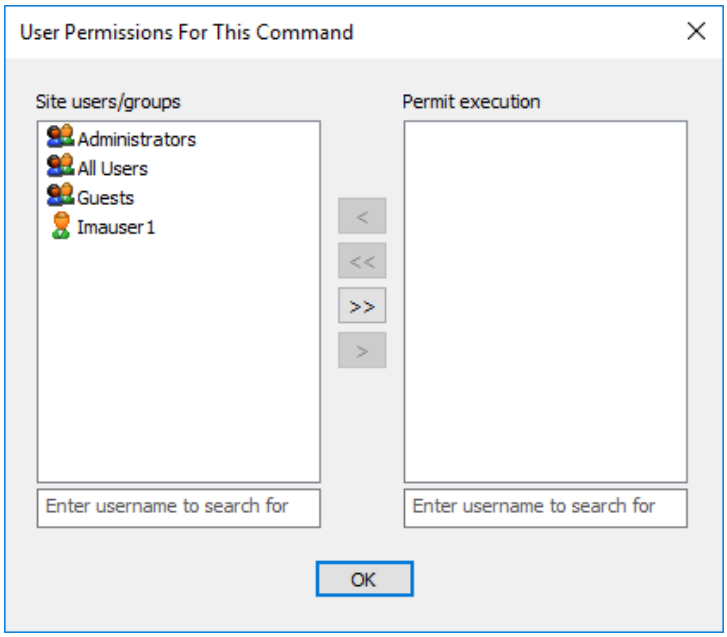
8. To create a log that you can use to troubleshoot the command in case of failure, select the **Redirect output to a log file** check box, then type the path to the log file or click the folder icon to browse to and select the file.
9. If you want EFT to return an error if the launched process fails to respond, select the **Enable process timeout** check box and specify the number of seconds the Server should wait before terminating the command.
10. To specify FTP client settings, in the **FTP Custom Command Specific** area, click **Configure**. The **FTP Custom Command Specific**dialog box appears.



11. Select the **Redirect command output to connecting client** check box if the command will be launched by a connecting FTP client. If you select **Redirect command output to connecting client**, the result is sent to the connecting FTP client in a 220 message response.
12. If you want to force the FTP client to send a minimum number of parameters, select the **Require a minimum of**check box and specify the minimum number of parameters required.
13. To provide a message that users will receive when the parameter number is not met, next to **Invalid parameter count message**, click **Configure**.



14. Provide the message, and then click **OK**.
15. To specify the users and Groups that can execute the Command, next to **User (s) or group(s) allowed to execute this custom command**, click **Configure**.



16. Double-click the users and/or groups, or use the arrows to move them between the **Site users/groups** list and the **Permit execution** list, and then click **OK**.
17. Click **Apply**to save the changes on EFT.

Related Topics

- Introduction to EFT Commands
- Viewing and Removing Commands
- Enabling and Disabling Commands

Custom Command Example

The following example Command shows the configuration of a custom Command from the perspective of both EFT and a client. To follow the example exactly, you will need to download and install CuteFTP, which is available as a free trial and can be downloaded from the website. However, any client that supports custom commands or raw FTP commands will work. The command example described below copies EFT log files from the **Logs**folder to **C:\Temp** using the Windows xcopy command and CuteFTP's command-line functions.

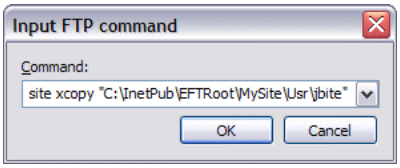
To create a custom Command

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, expand the Site node for the Site that you want to configure, and then click **Commands**.
3. In the right pane, click **New**. The **Custom Command Wizard** appears.
4. Follow the instructions in Creating a Command with the Custom Command Wizard to define a Command that uses **xcopy**.

You can run this command example "on the fly" in the FTP client (in this example, CuteFTP), or insert the Command in an Event Rule. Each of these methods is described below.

Using the Command "on the fly" in CuteFTP

1. Start CuteFTP, and create a connection to EFT. (Refer to the CuteFTP help for details of how to connect to a server.)
2. If not already displayed, open the **Session Log** pane. (On the main menu, click **View > Show Panes >Individual Session Logs** or press ALT+2.)
3. Right-click a blank area of the **Session Log**, then click **Input Raw FTP Command**, or press CTRL+SHIFT+I. The **Input FTP Command** dialog box appears.



4. In the **Command**box, type `site`, the name of the Command as defined in EFT and any required parameters. For this example, type:
   ```
   site xcopy "C:\InetPub\EFTRoot\MySite\Usr\jbite" "C:\Temp"
   ```
5. Click **OK**. The Command executes. In this example, each of the files in the **\Usr\jbite** folder was copied to the **\Temp** folder. If you selected the **Return output to client**check box when you defined the Command in EFT (step 8 above), the **Session Log** displays the results of the Command. For example:

```
COMMAND:> site xcopy "C:\InetPub\EFTRoot\MySite\Usr\jbite"
"C:\Temp"
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\cftpsaiProperties.gif
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\EFTtaxonomy_
filelist.xml
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\EFTtaxonomy_
image001.png
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\inheritance.doc
220-220-C:\InetPub\EFTRoot\MySite\Usr\jbite\Message3.gif
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\RE Certificate
Chaining.htm
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\Root Migration
Scripts.htm
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\Thumbs.db
220-8 File(s) copied
220-220-220 Command completed with code 0.
```

Configuring the Command in CuteFTP

1. Start CuteFTP and connect to EFT. (Refer to the CuteFTP help for details of how to connect to a server.)
2. On the main menu, click **Tools >Custom Commands >Edit Custom Commands**. The **Custom Commands** dialog box appears.

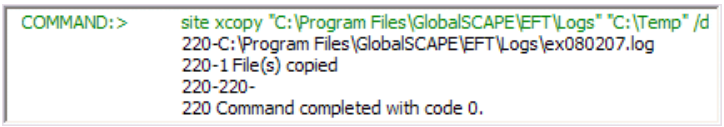
   You must be connected to an FTP server in order for the Commands option to be available.

3. Click **New** then type a name for the command. For this example, type `xcopy`.
4. Click the command in the tree, and then click **Edit** or right-click the new command and click **Properties**. The **Custom Command Properties** dialog box appears.
5. In the **Label**box, the name of the command appears.
6. In the **Command** box, type:

   ```
   site xcopy "C:\InetPub\EFTRoot\MySite\Usr\jbite" "C:\Temp" /d
   ```

   > **NOTE:** Commands must start with *site* and then the command name you used in EFT, not the name you gave the command in CuteFTP. The */d* parameter copies all new files in the specified folder.

7. Optionally, specify any key or key combination for the Shortcut Key and any icon for the **Toolbar Icon**.
8. Select the **Place on the Custom Commands toolbar**check box, and then click **OK** to close the **Custom Commands Properties** dialog box.
9. Click **OK** to close the **Commands** dialog box. Your custom command is now enabled and the icon, if specified, appears on the toolbar. (If the command is not displayed, click **View >Toolbars >Custom Commands Bar**.)
10. Start CuteFTP and connect to EFT.
11. If it not already displayed, open the **Session Log** pane. (On the main menu, click **View > Show Panes >Individual Session Logs** or press ALT+2.)
12. On the toolbar, click the Command icon that you just created.
13. Monitor the output in the **Session Log**. You should receive various response messages indicating the progress of the archive.



Executing the Command Automatically Using an Event Rule

If you want to copy the log file automatically every day, you can create a Scheduler (Timer) Event and insert the **Script: Custom Command**Action. Using this method, you would have to define the parameters in the **Execute Command** dialog box from within the Event Rule. See also Script: Custom Command Action.

Possible Error Situations

- If you repeat the hard coded parameters in both the client and EFT, then the first parameter that the client sends will be used. For example, if *SITE ZIP -c %at[archive name] %ff* is configured in the client, and *-c %1% %2%* is configured in EFT, then the first parameter (*-c*) that the client sends will be used as *%1%* and the resulting string would be `-c -c filename.ext`. Therefore, it is important to educate the FTP user on the proper syntax and supply most of the hard-coded parameters on the EFT side.
- You must give the FTP client user permission to run the Command on the **Permissions** tab on EFT; otherwise, they will receive a "Permission Denied" error.
- Certain command line utilities that may show a Windows prompt or other dialog may not execute properly when called from the FTP engine while it is running as a service. This is especially true when the service is logged in to from a Local System account.
- EFT can return an error if the client provides the wrong number of parameters or invalid parameters.
- To limit security vulnerabilities to EFT, the EFT administrator should only allow limited access to commands that launch processes.

  Always use caution when giving program access to your system32 directory (especially an FTP server).

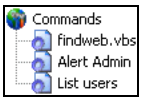
Viewing and Deleting Commands

Custom Commands defined on a Site appear in the left pane under the Commands node for the Site and in the right pane when the Commands node is selected. To create a command, refer to The Custom Command Wizard. On the **Commands List** tab, you can view, edit, delete, and add new Commands.

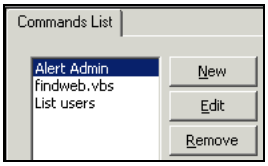
To view the Commands defined on a Site

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, expand the Site node for the Site that you want to configure, and then click **Commands**.

   The Commands appear under the **Commands**node.

   The **Commands List** tab appears in the right pane.

   Double-click a Command to view its properties.

To delete a command, do one of the following:

- In the right pane, click the Command in the **Commands List**, and then click **Remove**.
- In the left pane, click the Command, then press DELETE.
- In the left pane, right-click the Command, and then click **Delete**.

Related Topics

- Introduction to EFT Commands
- Creating a Command
- Enabling and Disabling Commands

Enabling and Disabling Commands

You can enable and disable Commands as needed, without deleting them. When you create a new Command, the **Enable this command** check box is selected on the **Command Settings** tab.

To enable or disable a Command

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, expand the Site node for the Site that you want to configure, click **Commands**, and then click a Command in the tree. The Command's definition appears in the right pane on the **Command Settings**tab.
3. To disable the Command, clear the **Enable this command** check box, and then click **Apply**. When the Command is disabled, an x within a red circle appears over the Command's icon.

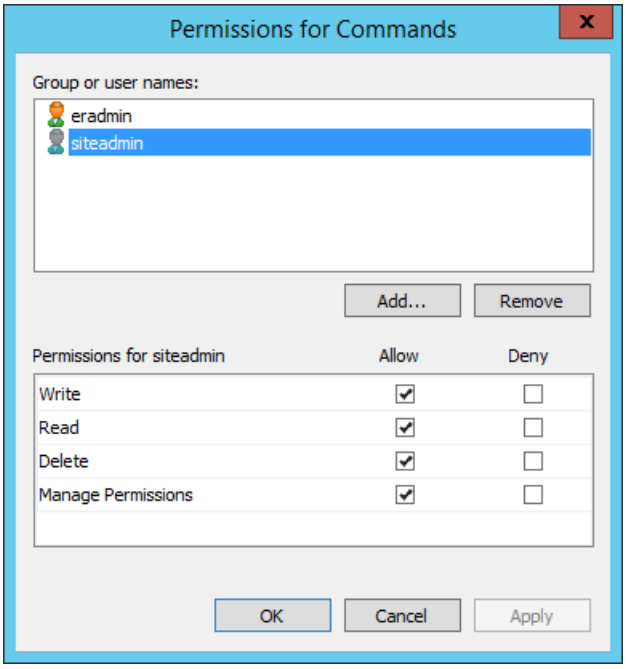
4. To enable the Command, select the **Enable this command** check box, and then click **Apply**. When the Command is enabled, the x within a red circle does not appear over the Command's icon.

Command Permissions

Certain delegated administratorshave all permission (Write, Read, Delete, and Manage Permissions) to manage the Custom Commands. Granular permissions allow the EFT administrator to control which administrators have control over certain objects. For example, you might want to give the Site administrator permission to Manage Permissions, but give the Event Rules administrator only Read permission.

To edit permissions

1. Right-click the **Commands**node or a specific command, then click **Permissions**.



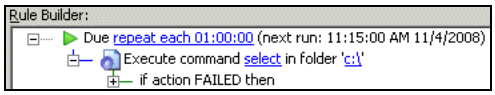
2. Clear the check boxes for the permission you do not want to assign; select the check boxes for the permissions that you want to explicitly **Allow** or **Deny**.
3. When you assign permissions at the Commands node, the permissions are inherited by the Commands. You can change the permissions for each of the Commands and for each administrator, if necessary.
4. Click **OK**.

Using the "Script: Custom Command" Action

(Require EAM) You can configure EFT to run executables, batch files, and scripts automatically when specific events occur. EFT calls these *Commands*. When the Event Rule is triggered, EFT executes the specified custom command and attributes.

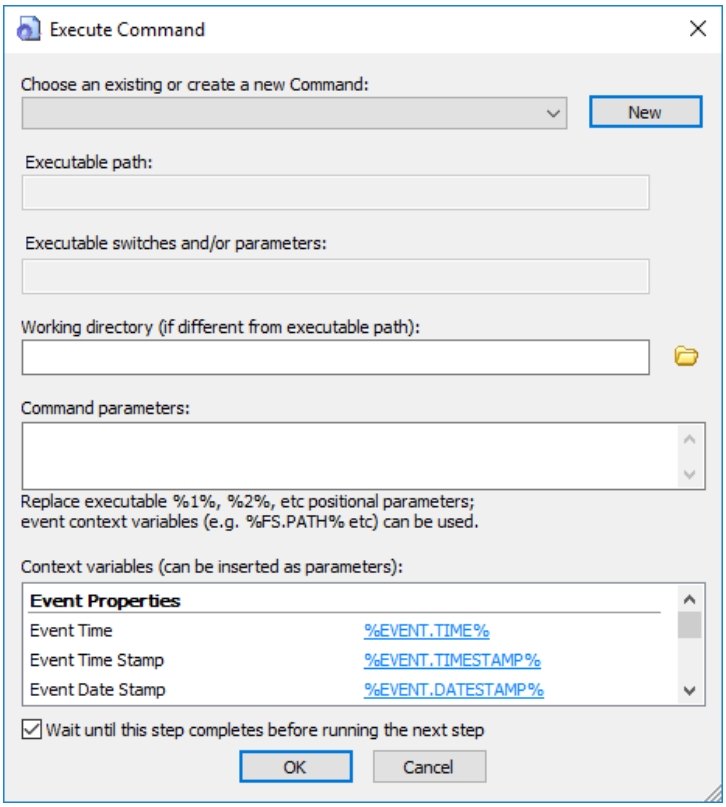
To execute a Command from EFT's Event Rule system

1. Identify the Command you want to execute with the Event Rule or create a new custom Command using the procedure in Creating a Command. Or you can create a new Command later from within the Event Rule (in step 6 below).
2. Open the Event Rule with which you want to execute the Command or create a new Event Rule using the procedure in Defining Event Rules.
3. (Optional) If you need to apply any conditional behavior, click it in the **Conditions**list.
4. In the **Actions**list, double-click **Execute command in folder**. The Action is added to the Event in the **Rule Builder**.



Links in the **Rule Builder** indicate parameters that must be defined to save the Rule.

5. In the **Rule Builder**, click one of the underlined text links. The **Execute Command** dialog box appears.



6. In the **Choose an existing or create a new Command** list, click the list to select the command. (If you did not create the Command in step 1, click **New** to create the Command now.)
7. The Executable path and Executable switches and/or parameters boxes display the path and switches for the selected Command. (If you want to change anything, you will have to close this dialog box, apply any changes to the Event Rule, go edit the Command, then reopen the Event Rule to continue defining it.)
8. In the **Working directory**box, type the path or click the folder icon to specify the folder in which the script or executable resides e.g., **C:\EFTscripts**. For mapped drives, use their UNC path. (File browse operations are disabled when you are connected remotely. You can't click the folder icon and browse, but you can type a path that is relevant to the EFT computer, not the remote interface).
9. (Optional) In the **Command parameters** box, include any parameters for the command.

   You can select items in the **Context variables** list to add them as parameters. For example, suppose you want to run a script on a file that was uploaded and triggered the Event Rule. You would type the script name and the tag `%FS.FILE_NAME%`, as shown below:

   ```
   dosomethingwithfile.vbs-file %FS.FILE_NAME%
   ```

   Refer to Variables for details of available variables and how to use them.

EFT passes the complete variable along to the Command; however, due to limitations of some command-line applications, they may not be able to interpret the Command properly. In certain instances, such as when there is a semicolon in a file name, you may need to enclose the variable in quotation marks in the **Command Parameters**box after you insert it from the Context variables box.

10. (Optional) The **Wait until this step completes before running the next step** check box is selected by default. When the check box is selected, you can select the "If failed" action, and populate it with actions to run in case the rule fails. To allow the next step to run before this action completes, clear the check box. If check box is not selected, a prompt appears to confirm: "This step will be executed asynchronously (non-blocking), which means EFT won't wait for this step to be completed before running the next step. This could yield undesirable results if the next step depends on the output or outcome of this one. Are you sure you want to make this action asynchronous?" (All actions in the IF FAILED section are lost if the parent action is switched from async to sync mode.)
11. Click **OK** to save the Command.
12. Add other Actions as needed, and then click **Apply**to save the Event Rule.

Example: Using a Command in an Event Rule to Copy Files

If you want to copy EFT's files to another location based on the date (for example, all log files created on a specified date), you can create a custom Command that points to the Windows XCopy command. The executable is (by default) in **c:\windows\system32\xcopy.exe**. Numerous switches are available for this command. (You can see all of the options by typing `xcopy /?` at a command prompt.) You must type the *source path* and the *destination path*.

You can add a switch, `/d:mm-dd-yy`, to copy files that were changed on or after a specified date. If no date is provided (just the `/d`with no date), it copies all source files that are newer than existing destination files. That is, it will not copy a file with the same name/same date or same name/older date.

To define an Event Rule to copy files, assuming that EFT has permissions to access the files, you can create a Folder Monitor Rule and specify that if the Condition "If File Change does equal to added" exists, then execute the Command to `xcopy`the newer files to the destination location.

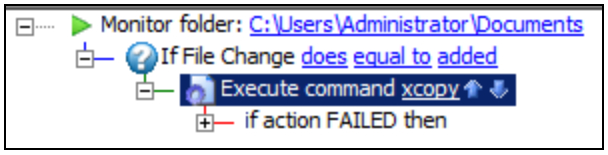
To define an Event Rule to copy log files

1. Create a custom command to execute the Windows Xcopy command. The executable is (by default) in **c:\windows\system32\xcopy.exe**.
2. In the **Working directory**box, type the path or click the folder icon to specify the folder in which the script or custom command executable resides (**C:\windows\system32**).
3. In the **Parameters**box, type the source folder (the location of the log files), the destination folder (the location to which to copy the files), and any other Xcopy parameters you need. For example, type:

   ```
   "C:\ProgramData\Globalscape\admin\Logs\*.log" "C:\Temp\" /d
   ```

   The parameters tell the Xcopy command to copy all **.log**files in the **EFT\Logs** directory to **C:\Temp**. The parameter **/d** (with no date) copies all source files that are newer than destination files.
4. Create a Folder Monitor Event Rule.
5. Add the Condition **If File Change equal to operation**, and then click **operation**to change it to **added**.

6. Add the **Execute command in folder** Action to the Rule, and then click **select**. The **Execute Command** dialog box appears.
7. In the **Choose an existing or create a new Command** box, click the XCopy Command that you defined in step 1.

8. Click **OK** to close the **Command Configuration**dialog box, and then click **Apply** to save the Rule on EFT.

The Rule is now defined to copy log files from the monitored folder (**C:\ProgramData\Globalscape\admin\Logs**) to the new location (**C:\Temp**). (Note that they are copied, not moved.)

You could also add an email Notification Action to let you know when the Command is executed.

Always use caution when giving program access to your system32 directory (especially an FTP server).

Script: PowerShell Action

(Requires EAM) The **Run PowerShell script** Action is used in Event Rules to execute a PowerShell script. (Requires Windows PowerShell 4.0 or later.)

EFT will always use Windows PowerShell ISE (if available on the target machine) to edit the embedded script, regardless of your default setting.

A PowerShell log is enabled and saved in the **\ProgramData** folder as **\Logs\powershell.log**.

100s of PowerShell functions and cmdlets are available. Refer to https ://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-date?view=powershell-7for cmdlets examples and information about using PowerShell.

VariantWrapper for variables to be passed as VARIANT will fail in PowerShell. (This is a bug in PowerShell.)

EFT context variables (where populated) need to be passed into the script. The script will access variables with `$EFT_CONTEXT`global variable via the `GetVariable` method. Create or modify context variables by using `SetVariable`method of `$EFT_CONTEXT`global variable.

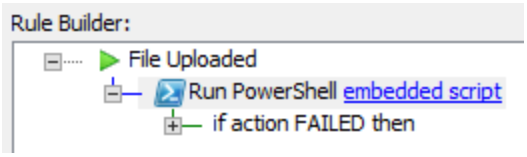
The script action is able to modify or create any variables except the systems environment (`%ENV.`) pseudo variables. When `%ENV.[value]%`is used in event rules, EFT will look up the [value] from the systems environment variables.

When referencing a dataset in PowerShell, PowerShell does not handle the % symbol, so this is how it would be accessed: ("Customer.CurrentRow.FirstName")

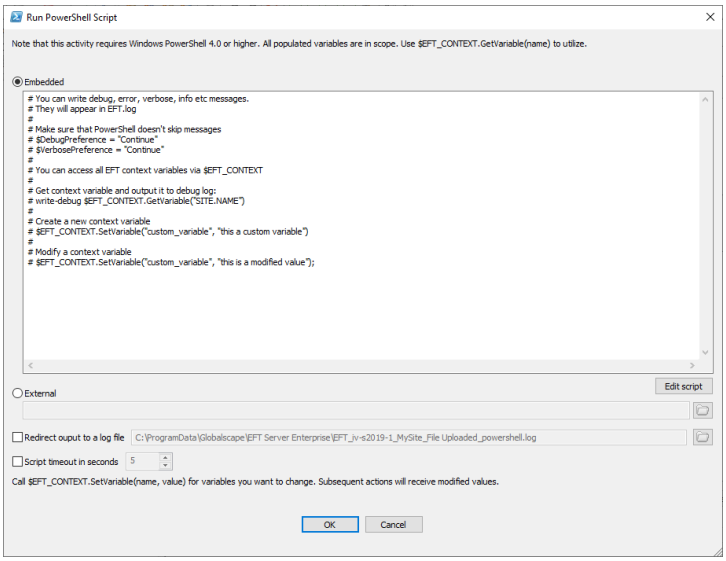
```
$EFT_CONTEXT.GetVariable("Customer.CurrentRow.FirstName") + ','
+
$EFT_CONTEXT.GetVariable("Customer.CurrentRow.LastName")
>>C:|Users\Administrator\Desktop\test
```

To user a PowerShell script in an event rule

1. In the administration interface, connect to EFT and click the **Server**tab.
2. Create a new Event Rule.
3. Add the **Run PowerShell script** Action to the rule.



4. In the Rule Builder, click the **embedded script** link. The **Run PowerShell Script** dialog box appears with a sample script that is commented out.



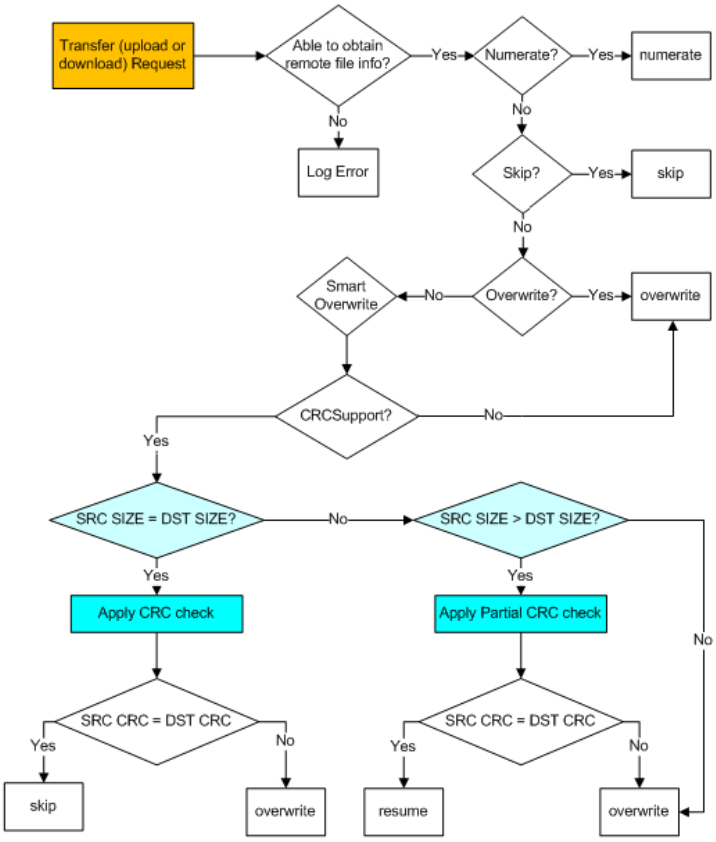
5. Click **Embedded**if you want to paste a script into the dialog box or click **External** of you want to point to a PowerShell script in a folder that EFT can access.
6. To create a PowerShell log file, select the **Redirect output to a log file** check box, then specify where to save the log. By default, it is saved to **C:\ProgramData\Globalscape\EFT Server\<computer_name>_<site_name>_<event_rule_name>_powershell.log**.
7. If you want to analyze PowerShell output in context with the event trigger and all associated actions with that event, you would need to clear the **Redirect** check box, apply changes, then open logging.cfg, un-comment the Event.PowerShell logger (remove the #), then save the logging.cfg file. (If you leave the **Redirect**check box selected, the PowerShell logs will not appear in logging.cfg for this action.)
8. Click **Edit Script**to view/edit the script in a text editor. (Windows PowerShell ISE is the default editor.)
9. Select the **Script timeout** check box and specify the number of seconds before terminating the script.
10. Click **OK** to save the action.
11. Add other conditions or actions as needed, then click **Apply** to save the rule.

Smart Overwrite

On the **Destination File Path**page of the Protocol Upload Action wizard, you can specify what EFT is to do if the file you are copying or moving has the same file name as a file in the destination path. Depending on what it detects, Smart Overwrite can overwrite the file in the destination path, skip the copy/move, numerate the copied/moved file, or overwrite the destination file after performing a CRC match of the files.

Smart file transfer is complex multi-step process in which intermediate steps are allowed to fail. Occasionally these intermediate steps that fail will cause ERRORs in the transfer log, yet the file transfer does succeed.

- **Overwrite =**Overwrite any existing file with the same name.
- **Skip =** Skip the offload if a file with the same name exists in the destination directory.
- **Numerate =**If a file in the destination folder has the same name as the file you are transferring, EFT renames the transferred file to "Copy of file.txt." If the same transfer occurs again, EFT renames the transferred file to "Copy (2) of file.txt" and so on.
- **Smart Overwrite =**EFT performs a CRC match of the files. (Supported only on FTP transfers.)
    - If the destination and source file sizes are the same, then the CRC determines whether it should skip the file or overwrite the file. If the file contents are identical, the destination file is not overwritten.
    - If the destination size is ***smaller***than the source size (meaning a partial file likely exists in the destination file path), then EFT will perform CRC on the portion of the source file that matches the length of the destination file. If the contents match, then EFT resumes the download. If they do not match, then the file is overwritten.
    - If the destination file size is ***larger*** than the source file, then EFT overwrites the file without performing CRC first.


Transfer (upload or download) Request
Able to obtain remote file info?
Yes
Numerate?
Yes
numerate
No
Log Error
No
Skip?
Yes
skip
No
Smart Overwrite
No
Overwrite?
Yes
overwrite
CRCSupport?
No
Yes
SRC SIZE = DST SIZE?
No
SRC SIZE > DST SIZE?
Yes
Yes
Apply CRC check
Apply Partial CRC check
No
SRC CRC = DST CRC
SRC CRC = DST CRC
Yes
No
Yes
No
skip
overwrite
resume
overwrite

System: Backup Action

A Backup Server Configuration Event Rule is defined and enabled by default to back up EFT configuration automatically on a recurring schedule. You can also run the wizard manually. For more information about the Migration wizard, refer to Backup Server Configuration Wizard.

IMPORTANT: If the Timer Event Module is not licensed, the default Backup Server Configuration rule will not function after the trial has expired.

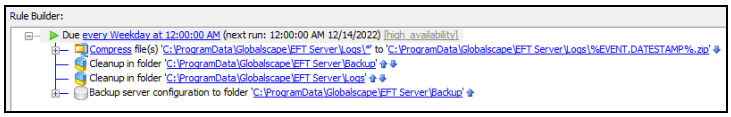
When you create your first Site, a new **Backup and Cleanup** rule is created that runs the System: Backup and System: Cleanup Actions once a day at midnight, using all defaults for naming and backup location. The default Rule includes a Cleanup Action to delete backup files (*.bak) older than 30 days in that same folder. The Rule is created and enabled when EFT is installed, but you can disable it and edit it as necessary.

> **NOTE:** You should specify a backup location that is not on the EFT server hard drive. If EFT's hard drive fails, you will need to use the backup to restore configuration. Ensure that EFT has permission to write to the folder that you specify for backup, especially if EFT is installed in a cloud location.

The default folder for backups, **C:\ProgramData\Globalscape\EFT Server\Backup**, is a hidden folder. In Windows File Explorer, click the **View** tab, then select the **hidden items** check box.

To create (or edit) the Backup Server Configuration Event Rule

1. Create a Rule using the Timer, Service Stopped, Server Started, Event Rule Subroutine, GDPR Exercised, or IP Added to Ban List Events. If you are using the Timer Event, click the "Due <link>" hyperlink to define the backup schedule in the **Timer Event** dialog box. Refer to Scheduler (Timer) Event for details, if necessary.
2. Double-click the **System: Backup** Action or click it, and then click **Add**. The Action is added to the Rule.
3. Click the hyperlink in the **Backup Server Configuration** Action. The **Browse for Folder** dialog box appears in which you can specify where to save the backup file. (Use a UNC path.) By default, the backup file is saved to the EFT's Application Data folder (for example, **C:\ProgramData\Globalscape\EFT Server\Backup**). You should change this location to a hard drive other than the one on which EFT is installed.
4. Click the folder icon to select the folder in which to save the backup file, and then click **OK**.
5. (Optional) Add the **System: Cleanup** Action to removed old backups. Refer to Clean-Up Action for details, if necessary. The default Rule is configured to delete **.bak** files that are older than 30 days. You can delete backups manually, if desired. Be sure to point to the location where the backup file is saved.
6. Add other Actions as needed, such as email notifications.
7. Click **Apply** to save the changes on EFT.
8. Click **Run Now** to test the Rule and verify that a file named "Server Configuration Backup <MM-DD-YYYY_HH-MM-SS>.bak" is saved in the assigned location.



The default **Backup and Cleanup** Event Rule includes a Compress files action and a Cleanup Action. Additionally, a Cleanup action is added to clean up the Logs folder. If you do not want to save logs created by LAN transfers, you can disable the logs using an advanced property. Refer to Event Rules Client Log for more information.

System: Cleanup Action

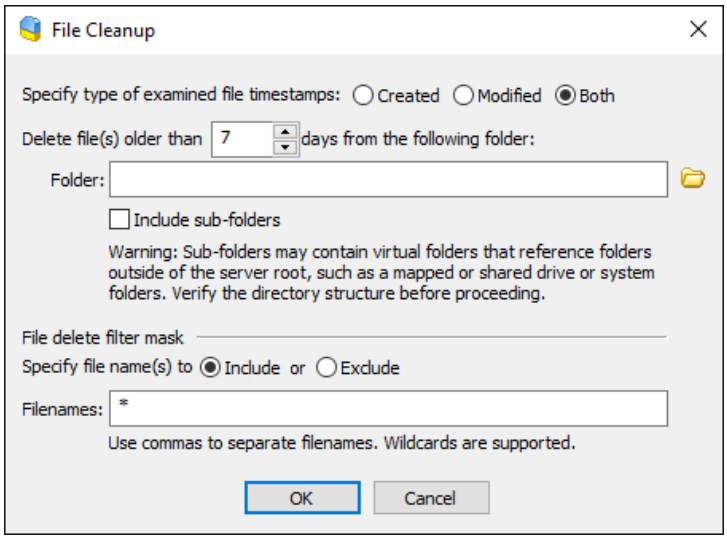
When you create your first Site, a Timer Rule is created that runs the System: Backup Action once each day at midnight, using all defaults for naming and backup location (\backup\Server Configuration Backup [Month] [Day] [Year].bak). The Rule includes a **Cleanup** Action to delete backup files (*.bak) older than 30 days in that same folder and another Cleanup in folder Action to remove old log files. This Backup and Cleanup Rule is enabled by default, but you can disable it and edit it as necessary. **After the trial expires, you should license the Timer Event module to continue backup/cleanup on a schedule.**

The **Cleanup** Action is available with the Scheduler (Timer), Event Rule Subroutine, Folder Monitor, GDPR Exercised, IP Added to Ban List, and REST Invocation, Events.

At the interval that you specify, EFT compares the filter parameters of the Cleanup in folder Action to the files in the designated folder, then determines the creation or modification time of the file and deletes ("cleans up") files that match the cleanup parameters. For example, if you specify to cleanup files that are older than 7 days named **dailyreport*.doc** in the folder **D:\WorkFolder\Sales\Daily Reports**, any Microsoft Word files in that folder with **dailyreport** in the file name are deleted after 7 days. However, if you create a Cleanup in folder Action and set a file to be cleaned after 7 days, but then modify the file on the 6th day, the file will not be deleted until 7 days after the modification date.

To configure EFT to cleanup files automatically

1. Follow the procedure in Creating Event Rules to create a **Scheduler (Timer) Event**. The Event Rule appears in the **Rule Builder**.
2. In the **Actions** list, double-click **Cleanup in folder**. The Action is added to the Rule in the **Rule Builder**.
3. In the **Rule Builder**, click the **'[select]'** link. The **File Cleanup Action Parameters** dialog box appears.



4. Specify which type of file timestamps you want to delete: **Created** time, **Modified** time, or **Both** created and modified times.
5. In the **Delete file(s) older than <n>** box, specify the minimum age of a file to delete from the folder. The default is 7 days.
6. In the **Folder** box, click the folder icon to specify the folder that you want to clean up.
7. To clean up subfolders in the specified folder, select the **Include sub-folders** check box.
8. If you don't want to delete all of the files older than a certain age, create a **File delete filter mask**. In the **Filenames** box, an asterisk appears by default, which means delete all files. You can **Include** or **Exclude** specific files from the **Cleanup in folder** Action, and/or use wildcards for file types, partial names, and so on.

   For example, the **Backup and Cleanup** Event Rule that is defined automatically in EFT is configured to delete all *.bak files in **C:\ProgramData\Globalscape\EFT Server\Backup** that are older than 30 days.

   Or, maybe you want delete everything in the folder except for the files with "new" in the file name. To do that, you would click **Exclude** and then in the **Filenames** box, type ***new***.
9. Click **OK** to close the dialog box.
10. Click **Apply** to save the changes on EFT.

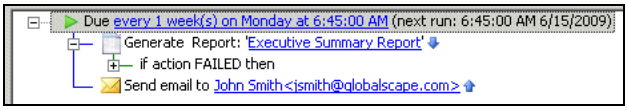
System: Report Action

(Requires ARM) When the Auditing and Reporting module is activated, you can configure an Event Rule to generate a report, then email it or save it to a file. If you add the Generate Report Action to a Rule, you must also tell EFT what to do with the report (save it or email it or both). When a report is generated by the Generate Report Action, a temporary, enumerated copy of the report is created and stored locally in the EFT installation folder. The temporary copy is deleted once the Event Rule context is out of scope.

To facilitate compliance with PCI DSS requirement 10.6, EFT automatically generates a report of PCI/High Security-related configuration and functions. The report is converted to HTML and then emailed or saved to a file specified by the EFT administrator.

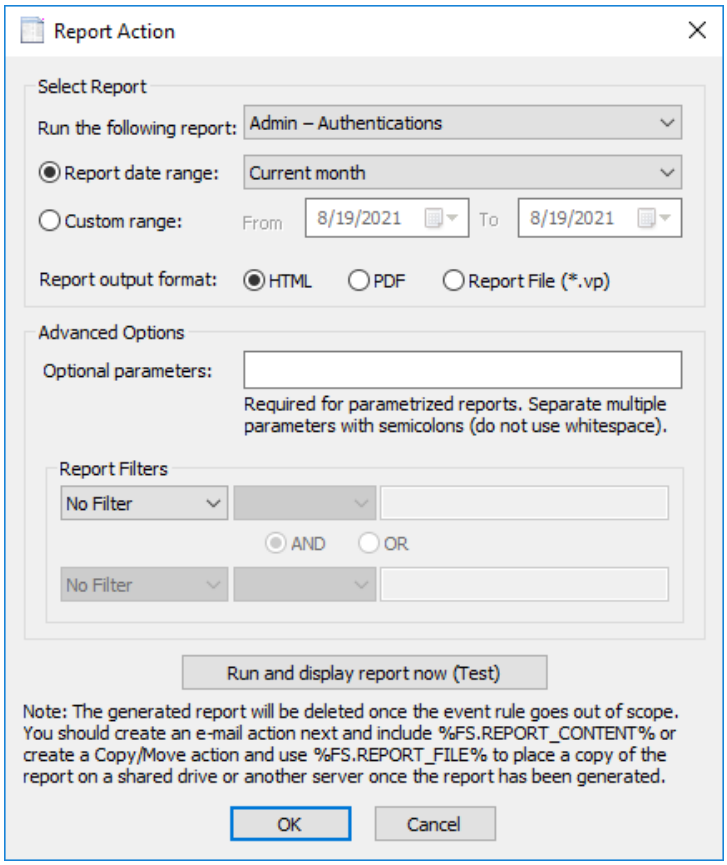
The automatic **Generate Report**Action never prompts for parameters because it will be run from the service on a timer, and thus does not allow interaction by a user. Reports that require parameters but do not have sufficient administrator-defined parameters will not run.

Example of a Report Event:



To create an Event Rule with the Generate Report Action

1. Follow the procedure in Creating Event Rules to create a new Rule, or select the Rule to which you want to add the Action.
2. In the **Actions** list, double-click **Generate Report**, or click it, and then click **Add Action**. The **Report Action** dialog box appears.



3. In the **Run the following report** box, click the down arrow to select a report from the Reports directory. (Custom reports also appear in the list.) Refer to Descriptions of Preconfigured Reports for a description of the Globalscape-defined reports.
4. Click **Custom range**to specify a custom date range in the **From**and **To** boxes or click **Report date range** and click the drop-down list to specify one of the following options:
    - **Include all dates**. If the selected dates include future transactions (for example, if the ending date for the report is today's date), the future transactions will not appear in the report.
    - **Today**. From 00:00:00 to the current time.
    - **Yesterday**. The previous day from 00:00:00 to 00:00:00.
    - **Last 24 hours**. The previous 24 hours from the current time.
    - **Month to date**; **Quarter to date**; **Year to date**. Starting from the first day of this month, quarter, or year, and ending today. (Quarters begin January 1, April 1, July 1, and October 1.)
    - **Current week**; **Current month (default)**; **Current quarter**; **Current year**. Starting from the first day of this week, month, quarter, or year, and ending with the last day of this week, month, quarter, or year. (Quarters

begin January 1, April 1, July 1, and October 1.)

- **Last week**; **Last month**; **Last quarter**; **Last year**. Starting from the first day of last week, month, quarter, or year, and ending with the last day of last week, month, quarter, or year. (Quarters begin January 1, April 1, July 1, and October 1.)
- **Last 30 days**. Starting from 30 days ago, and ending with today's date.
- **Last 12 months**. Starting 12 months ago from today's date, and ending with today's date. For example, if today is July 2, 2007 and this date range is selected, the report would run from July 2, 2006 through July 2, 2007.

5. In the **Report output format** area, specify the format of the report output: HTML, PDF, or VP (report file).
6. In the **Advanced Options**area, specify **Optional parameters**(separated by semicolons) for the report, which are evaluated from left to right. You can specify Event Rule variables. For example, if the report definition chosen in the **Run the following report** box requires two parameters for filename and username (in that order in the report definition), then the **Optional parameters** box can be populated with `*.txt;myname`to specify a filename parameter of `*.txt`and a username parameter of `myname`.
7. In the **Report Filters**area, specify filters with AND or OR. Available filters depend on report selected. (If you test the report and do not see the desired results, adjust your filters.)
8. To run the report in real time to verify that the Action was configured correctly, click **Run and display report now (Test)**.
9. Next, you should create an email Action and include the %FS.REPORT_CONTENT% variable or create a Copy/Move Action and use the %FS.REPORT_FILE% variable to place a copy of the report on a shared drive after the report has been generated.

   The variable %FS.REPORT_CONTENT% can be added to email notifications. When %FS.REPORT_CONTENT% is added to the body of email notifications, the content is displayed inline in the email in HTML format. (You must specify the HTML format in the **Report output format** area,)

The variable %FS.REPORT_FILE% can be used in copy/move, OpenPGP, and Custom Command Actions that have a failure Event defined, but should not be used for Actions that do not have a failure Event defined. Instead, use %FS.REPORT_CONTENT% for email notifications, because this variable represents a copy of the contents of the file rather than a link to the file, which is only good so long as the file exists. For a complete list of EFT variables, see Variables. Do not use %FS.REPORT_FILE% in email notifications.

Related Topics

- Using Actions
- Creating Event Rules
- Event Timer Rule

User Action

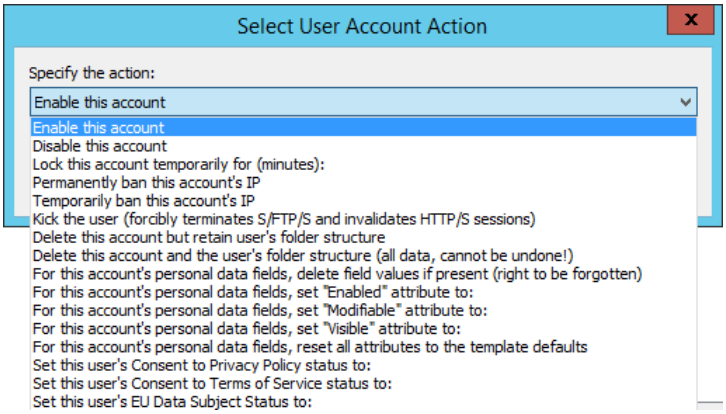
The **User** Action can be added to applicable Event Rules to perform actions such as disabling/locking the account, banning the account, and so on. The Action is ***not*** available for triggers associated with operating system events: Timer, Folder Monitor, Cloud object monitor, Server, and Site events.

(Available Actions contains a table of which Actions are available with which Event Triggers.)

The **User** Action is useful for things like compliance requests in which users might ask that an organization remove all traces of their account (for example, HIPAA, GDPR) .

To specify User Actions

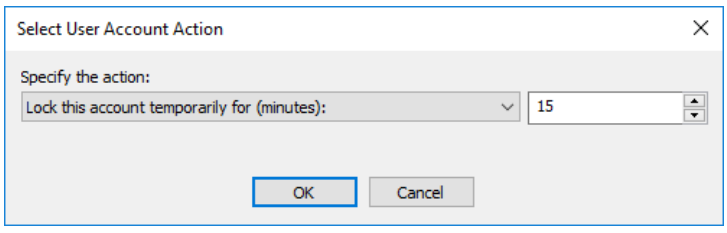
1. After you create an Event Rule, add any applicable Conditions and then add the User Account Action.
2. In the Event Rule, click the link in the Action to specify an Action. The **Select User Account Action** dialog box appears.



Actions (named for their specific function) include:

- Enable this account
- Disable this account
- Lock this account temporarily for (minutes)

  When you choose **Lock this account temporarily for (minutes)**, a field appears in which you can specify up to 15 minutes.



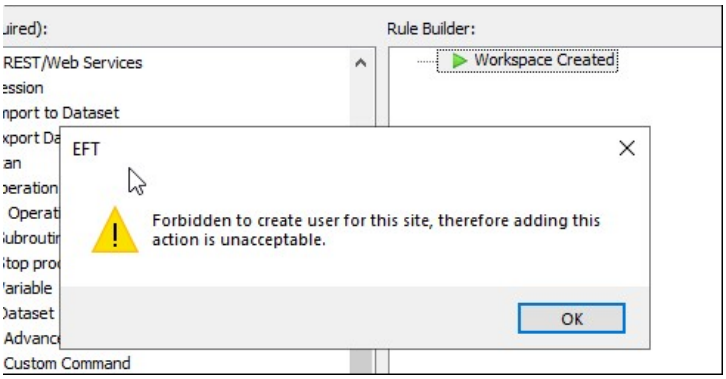
- Permanently ban this account's IP
- Temporarily ban this account's IP
- Kick the user (forcibly terminates SFTP, FTP, and FTPS, and invalidates HTTP and HTTPS sessions)
- Delete this account but retain user's folder structure
- Delete this account and the user's folder structure(removes all data and cannot be undone)
- For this account's personal data fields, delete field values is present (right to be forgotten)
- For this account's personal data fields, set "Enabled" attribute to: True, False
- For this account's personal data fields, set "Modifiable" attribute to: True, False
- For this account's personal data fields, set "Visible" attribute to: True, False
- For this account's personal data fields, reset all attributes to the template defaults.
- Set this user's Consent to Privacy Policy status to: Unknown, Granted (implicit), Granted (explicit), Denied, Rescinded
- Set this user's Consent to Terms of Service status to: Unknown, Agreed (implicit), Agreed (explicit), Disagreed, Withdrawn
- Set this user's EU Data Subject Status to: Unknown, Yes, No

3. Click **OK** to save the Action.
4. Add any other Actions, as needed, then click **Apply** to save the Event Rule.

User Create Action

On Globalscape-authenticated and ODBC-authenticated sites, you can add the **User: Create** action to an event rule when you want a certain event to trigger the creation of a new user. This action is available to any event trigger.

NOTE: If you try to add the **User: Create** action to an event rule on an LDAP-authenticated or AD-authenticated site, EFT will present the error message "Forbidden to create user for this site":



Event Rule Administrators are not able to create or edit event rules with the User: Create action. This behavior is by design; Event Rule administrators are not able to create users. An error message will be presented in the interface when attempting to perform this action.

When you click the **select** link, the **New User Creation** wizard appears in which you can add variables to populate the user definition. Context variables are available in the following fields: **Login**, **Password**, **Email**, all fields in the **User Account Details** dialog box, and the **Home folder** path (on the second page of the wizard).

NOTE: If the user name already exists, the "create" action will fail and the error is logged in the EFT log file. No error is displayed in the interface.

You can also onboard new users via a form that feeds into a tool such as "Service Now." Service Now then invokes REST API and passes in numerous parameters, such as username, password, and so on. (Service Now is not a Globalscape product. For Service now help, please contact Service Now customer support.) Refer to RESTAPIExamples (ZIP file) for an example of creating a user with the REST API. Refer to Creating a User Account for more details of account creation.

Using Wildcards with Event Rule Actions

The **OpenPGP** Action, the **Copy/Move** Action, and the **File Name** Condition support the use of wildcards. This is useful for Event Rules that batch process groups of files. Standard Windows/DOS format wildcards are used, such as **.file extension, search term* .???, *search term* ?.*, *.*, and so on. This functionality is particularly useful with the Timer Event.

Wildcards with OpenPGP

In the OpenPGP Action configuration dialog, the **File to Process** field supports wildcards. Each matching file is acted upon according to the Action definition.

Wildcards with Copy/Move

In the **Offload Action** wizard, the **Source** path field on the **Target File** tab supports wildcards.

When a wildcard is specified here, the **Destination** path field specifies the target folder to which each matching file is moved or copied. The files moved or copied into the destination file are given the same name as the files from the source. For example:

Source:

```
c:\test\*.txt
```

Destination:

```
/%FS.FILENAME%
```

Here, each "*.txt" file that is uploaded goes to "/", with a matching file name. Note that the destination file name is not overwritten.

Configuration Notes

- If the **source** of an Action is specified as a wildcard without any path information, the path defaults to the folder with the Event Rule that triggered this Action (for example, there is a "%FS.PATH%" variable for an **On Upload** Event.) If there is no folder like that available (for example, if the Event is an **On Timer** Event) the current working directory of the application is set as the source of the wildcard patterns. Typically, that is the installation directory of the application.
- When you define a wildcard in the source path for a Copy/Move Action and the protocol type is set to Local (Local Files or LAN), EFT respects Windows path syntax:

For example:

Source:

```
c:\Work\Today\*.*
```

Destination:

```
g:\Backup\Work\Today\
```

You can also use \\Work, if appropriate.

- The Destination Path (Upload Event target file as:) ignores any path information you enter after the trailing backslash. So if you type:

```
g:\Backup\Work\Today
```

EFT disregards "Today" and executes the move/copy into:

```
g:\Backup\Work\
```

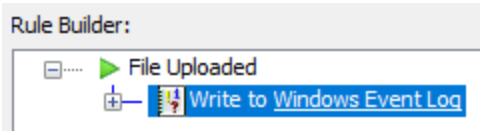
Test an Event Rule using a wildcard before you deploy it to ensure it works as expected and does not cause any unwanted behavior. For example, if you do not define the source path appropriately when a wildcard is used, it is possible to set up an Action that moves all the files out of a user's c:\windows directory, which is most likely an undesired result.

Example: Using Wildcards in Event Rules to Download from WinSSHD

Refer to the Globalscape Knowledgebase topic #10569for information about sending an email notification when a certain user uploads a file.

Windows Event Log (WEL) Action

The **Windows Event Log**Action is available for all Event Triggers to write to the Event Viewer. When you add the **Windows Event Log**Action to the **Rule Builder** and then click the hyperlink in the Action, the **Windows Event Log** dialog box appears. Use this dialog box to specify the WEL message parameters.

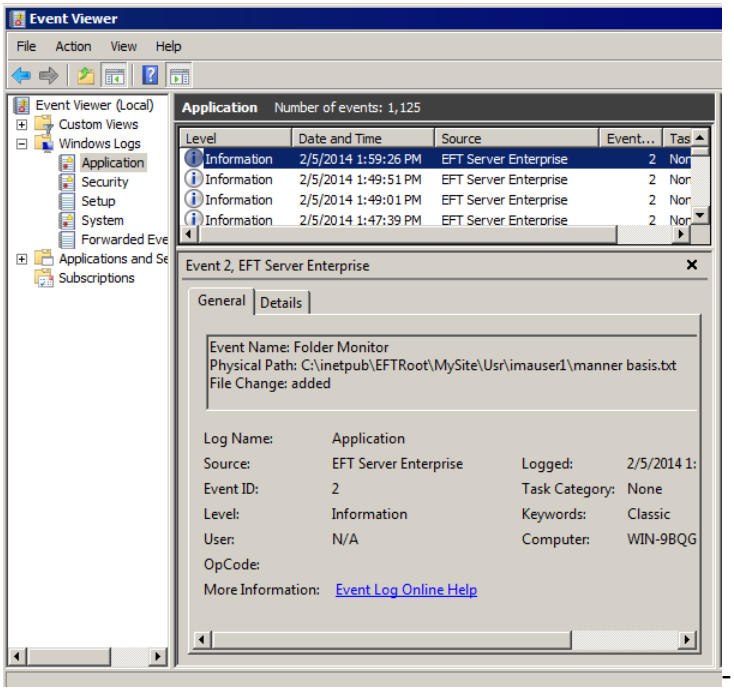


To configure the WEL message

1. In the **Type**box, click the down arrow and specify whether the message is an **Information**, **Warning**, or **Error** message. The default is Error.
2. In the **Event ID**box, click the up or down arrows to specify a number to assign to the Event, from 1 to 99,999 (defaults to 2).
3. In the **Description**box, provide a text description that will appear in the WEL when the Event is triggered, up to up to 2048 characters. By default, the message is whatever you have specified in the **Variable list**.
4. (Optional) In the **Variable list** box, click an EFT context variable to appear in the message. You can add multiple variables. The value of the variable will appear in the message when the Event is triggered.
5. Click **OK** to save the parameters in the Action.

To view the Windows Event Log

1. Click **Start > Run**.
2. Type `eventvwr.msc`, then press ENTER. The **Event Viewer**appears.
3. Click **Windows Logs > Application**. Double-click an EFT (Source) event. The **General** description and **Details** of the Event appear.



4. Notice that the description area displays the values of the variables that you provided in the **Windows Event Log Message** dialog box. In this example, we used the Event Name, Physical Path, and File Change variables. (Date and time are provided in the Event Viewer.)

Conditions

The topics below provide information regarding defining and using Event Rule Conditions.

- Using Conditions
- Condition Placement
- Changing Condition Placement
- Condition Evaluation
- Else Clauses
- Logical Operators
- Evaluating Expressions
- Compound Conditional Statement
- Event Properties
- Advanced Workflow Conditions
- AS2 Conditions
- Connection Conditions
- File System Conditions
- Remote Agent Event Rule Conditions
- Server Conditions
- User Conditions
- Workspaces Conditions

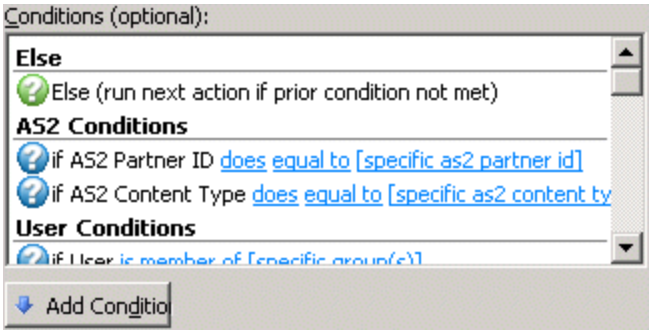
Using Conditions

Conditions allow you to define more narrowly the trigger for an Event Rule. Conditions are optional; you do not have to define a Condition on an Event Rule to make it trigger an Action, but Conditions allow fine control over when an Action can take place.

You can further fine-tune each Event trigger to execute only if certain Conditions are met. These optional Conditions act like filters or compound IF statements so that IF a specific Event occurs and IF a Condition is met, then an Action is executed. For example, an Event trigger that is called whenever a file is uploaded can be fine-tuned to trigger only if that file's extension is **.txt**and nothing else.

To add a Condition to a Rule

1. Create the Rule. In the **Conditions** list, the Conditions available for the selected Event appear. When applicable to the Rule, the **Else**option also appears.



2. Double-click a Condition in the list or click the Condition, and then click **Add Condition**.
3. Complete the Rule by adding one or more Actions, and then click **Apply**to save the Rule.

Conditions are NOT REQUIRED for an Event Rule to work. In its base form, the Event trigger itself is a sort of Condition, therefore you can execute Actions when/if an Event triggers, without adding any additional Conditions.

Conditions are organized by type:

- Advanced Workflow Conditions—Event is triggered based on Advanced Workflow criteria such an error.
- AS2-related Conditions—Event is triggered based on criteria such as protocol or AS2 ID.
- Connection Conditions—Event is triggered based on connection information such as remote IP or if user connected via the Java-enabled Web Transfer Client
- Context Variable Condition—Event is triggered when a context variable equals or doesn't equal a specified string.
- Event Properties—Event is triggered based on a specific Event reason.
- File System Conditions—Event is triggered based on criteria such as file size or virtual path.
- Server Conditions—Event is triggered based on criteria such as whether EFT is running or log name.
- Site Conditions—Event is triggered based on whether the Site is started or stopped.
- User Conditions—Event is triggered based on criteria such as whether the user account has a particular protocol enabled or login name.
- Workspaces-related Conditions—Event is triggered based on Workspace variables, such as folder owner.

Each of the available Conditions and which Events they can be used with is described above. There are no Conditions available for the **Site Stopped** or **Site Started**Events.

Related Topics

- Condition Placement
- Changing Condition Placement
- Condition Evaluation
- Else Clauses
- Logical Operators
- Evaluating Expressions
- The Compound Conditional Statement
- List of Conditions

Condition Placement

Where Conditions are placed within the **Rule Builder** when they are added depends on which item is selected in the **Rule Builder**.

- When the Event Rule *trigger*(the very first item in the **Rule Builder**) is selected and a Condition is added, the Condition is placed directly beneath the Event Rule Trigger. This is considered a "root" level condition.

```
ON FILE UPLOAD
{
  if ( %FS.FILE_NAME% = "*.pgp" )
//a root level condition. No action added yet
}
```

- When an Action inside another Condition is the selected item and a new Condition is added, that new Condition is placed directly beneath the Action and to the left, or outside of the container Condition. Otherwise, it would become a nested Condition, which EFT does not support.

```
ON FILE UPLOAD
{
 if ( %FS.FILE_NAME%  = "*.pgp" )
{
  PGPDecrypt %FS.FILE_PATH%
}
if ( %FS.FILE_NAME% = "" )
//new condition added placed at root level
{
```

- When an Action (that is not contained within a Condition) is the selected item, and a new Condition is added, the new Condition is placed immediately beneath that Action, at the same root level (see above example).
- When a Condition is the currently selected item and another Condition is added, the new Condition is ANDed to the selected Condition. If the Condition being added is the same Condition as the one selected, the new Condition is ORed to the selected condition. Using this method, you can create compound Conditions.

```
ON FILE UPLOAD
{
    if (%FS.FILE_NAME% = "*.pgp" ) AND (%FS.FILE_SIZE%
<300,000b)
    //a compound condition
```

```
        {
            PGP Decrypt %FS.FILE_PATH%
        }
    }
```

Related Topics

- Using Conditions
- Changing Condition Placement
- Condition Evaluation
- Else Clauses
- Logical Operators
- Evaluating Expressions
- The Compound Conditional Statement
- List of Conditions

Changing Condition Placement

When you have multiple Conditions, you can change the order by clicking them using the up/down arrows next to the Condition, at the bottom of the Rule Builder, or by using copy/paste. When a Condition is moved, the Condition and any actions inside of that Condition also move. If a Condition has an else statement under it, the else statement is also moved. This is because the Condition, any actions inside that Condition, and any attached Else clauses are considered a conditional block, and the entire block is moved.

Example:

Condition A

Action 1

Action 2

Condition B

Action 3

Click the Condition A down arrow ONCE, and Condition A and its child Actions are moved as a block:

Condition B

Action 3

Condition A

Action 1

Action 2

This same behavior does not apply when the Condition being moved is part of a compound Condition. To move one of the Conditions inside of a compound Condition down (or up), and, therefore, outside of that conditional block, you need to click on one of the Condition's up/down arrows:

Condition C1 and C2

Action 1

Action 2

Condition C3

Action 3

To move C1 down, click on the down arrow to the right of C1:

Condition C2

Action 1

Action 2

Condition C1

Condition C3

Action 3

To move a compound Condition, you need to select the ENTIRE Condition by clicking and dragging the Condition icon at the far left of the Condition, or select the line and then click the blue down arrow at the bottom of the dialog box (not the down arrow to the right of the Condition). A page icon appears if you drag it to an applicable location.

Related Topics

- Using Conditions
- Condition Placement
- Condition Evaluation
- Else Clauses
- Logical Operators
- Evaluating Expressions
- The Compound Conditional Statement
- List of Conditions

Condition Evaluation

Regardless of placement, ALL Conditions are evaluated, because all Conditions exist at the root level.

For example:

```
ON FILE UPLOAD
{
  if (%FS.FILE_NAME% = "*.pgp")
  //if filename extension is PGP then decrypt it
  {
    PGP Decrypt %FS.FILE_PATH%
  }
    if (%FS.FILE_NAME% = "*.zip") //even if the prior condition
was true, still evaluate this condition.
   {
   UNZIP %FS.FILE_PATH% to "%FS.FILE_
PATH%\%EVENT.DATE%_%EVENT.TIME%\"
   }
}
```

Related Topics

- Using Conditions
- Condition Placement
- Changing Condition Placement
- Else Clauses
- Logical Operators
- Evaluating Expressions
- The Compound Conditional Statement
- List of Conditions

Else Clauses

The Else clause or statement is a type of Condition and appears in the **Conditions** list box when at least one Condition has been added to the **Rule Builder**. The Else clause executes if the Condition preceding the Else statement is not met.

This is your typical Else statement as part of an IF/THEN/ELSE block:

```
If A Then

{ Run B }

Else >

{ Run C }
```

An Else statement must always follow a Condition. Else statements cannot be moved around independently. If you want to move the else statement, you need to move the entire conditional block or delete the else statement and re-create it elsewhere.

Below is an Event Rule example of using an Else clause.

Only the last Condition is considered before the ELSE statement is evaluated. That is, the ELSE statement will be TRUE only if the last Condition is FALSE, even if the preceding Conditions are TRUE.

Related Topics

- Using Conditions
- Condition Placement
- Changing Condition Placement
- Condition Evaluation
- Logical Operators
- Evaluating Expressions
- The Compound Conditional Statement
- List of Conditions

Logical Operators

When a Condition is added to another compound conditional statement, the newly added Condition will be ANDed to the Condition already present:

Example 1:

```
If Filename = bob.txt
```

Now add another Condition:

```
If Filename = bob.txt and If Filesize < 100 MB
```

When the second Condition being added is the SAME Condition type as the previous one, the newly added Condition will be ORed to the previous Condition.

```
If Filesize < 200 MB
```

Now add another same Condition:

```
If Filesize < 200 MB or If Filesize > 500 MB
```

If there are more than two Conditions already existing in a compound Conditional line, and another Condition is added (regardless of Condition type), the new Condition will use the same logical operators that are already present for that compound statement.

```
If Filesize < 200 MB or If Filesize > 500 MB
```

Now add another same Condition:

```
If Filesize < 200 MB or If Filesize < 400 MB or If FileName =
rob.txt
```

You can change the AND and OR operator values by clicking the **and** or the **or** hyperlink. Please note that logical operators separating conditional statements must be the SAME across the entire compound statement. You cannot mix and match AND and OR statements. When changing the logical operator for a compound conditional statement, ALL subsequent logical operators for that statement also change to match that operator. This is necessary to prevent problems with evaluation precedence, especially in conditional blocks with more than 2 conditional expressions to evaluate. There are ways around this limitation, discussed in Evaluating Expressions.

Example 2:

```
If Filename = bob.txt
```

Now add another Condition:

```
If Filename = Bob.txt and If Filesize < 100 MB
```

Now add another Condition:

```
If Filename = Bob.txt and If Filesize <100 MB and If group is
one of administrators
```

Now click one of the AND hyperlinks to change it to OR. The Conditions change to:

```
If Filename = Bob.txt OR If Filesize <100 MB OR If group is one
of administrators
```

Example 3:

```
If Filesize is < 200 MB
```

Now add another Condition:

```
If Filesize < 200 MB or If Filesize > 500 MB
```

Now click the OR hyperlinks to change it to AND. The Conditions change to:

```
If Filesize < 200 MB and If Filesize > 500 MB
```

With the AND in this example, the statement will never evaluate to true. You must change the comparison types or the comparison values, or switch back to the OR logical operator to avoid creating expressions that can never evaluate to true.

Related Topics

- Using Conditions
- Condition Placement
- Changing Condition Placement
- Condition Evaluation
- Else Clauses
- Evaluating Expressions

- The Compound Conditional Statement
- List of Conditions

Evaluating Expressions in Event Rules

EFT will always evaluate expressions from left to right, regardless of how many conditional checks there are within that same expression. One exception to this is described below.

Certain Conditions are able to test multiple values, such as the **If User is Member of** Condition or the **If Filename is one of** Condition. These Conditions are evaluated first and independently, with the resulting atomic unit evaluated as part of the complete expression.

For example, the **If User is Member of** Condition allows you to select from a list of Server Groups, therefore, the **If User is member of** expression is evaluated first, after which the rest of the expression is evaluated from left to right.

Related Topics

- Using Conditions
- Condition Placement
- Changing Condition Placement
- Condition Evaluation
- Else Clauses
- Logical Operators
- The Compound Conditional Statement
- List of Conditions

Compound Conditional Statement

```
If Filename (F)= Bob.txt AND If User is Member of administrators
(MA), Users (U), Power Users (PU)
```

If this expression were evaluated from left to right, the results would not match our expectations:

```
If (((F and MA) or U) or PU)
```

Instead, EFT evaluates the conditional statement first as its own atomic unit and then evaluates the resulting expression from left to right:

```
If (F and (MA or U or PU))
```

This allows you to create expressions that contain order-of-precedence grouping without having to use parentheses. The evaluative OR statement is hidden inside the conditional statement, as long as that conditional statement can evaluate against multiple criteria.

Only the following Conditions can evaluate against multiple criteria (strings):

• If User is Member of • If Login name • If Virtual Path • If Physical Path • If Physical Folder Name	• If Physical Destination Path • If Physical Destination Folder Name • If Destination File Name • If Virtual Destination Path • If Filename

To define multiple criteria for a Condition

1. Double-click a Condition in the list to add it to the Rule Builder. (To learn more about available conditions, refer to Conditions.)
2. If you are adding an additional Condition, highlight the existing Condition in the Rule Builder, then in the **Conditions** list, double-click the Condition you want to add. The Condition appends to the existing one and adds a logical operand (AND/OR).

3. Click the logical operand to change it.

   You can insert multiple Conditions. That is, you can have Condition 1 **AND** Condition 2 **OR** Condition 3.

If you need to use more complex criteria using AND and OR, you can use wildcard logic to create any logic that wildcards support. For example, if you add the **File Name** Condition to the **Rule Builder**, you can then define the path mask using complex logic with wildcards.

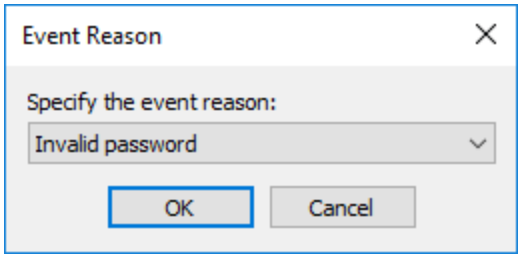
Related Topics

- Using Conditions
- Condition Placement
- Changing Condition Placement
- Condition Evaluation
- Else Clauses
- Logical Operators
- Evaluating Expressions
- List of Conditions

Event Properties

Event Properties are used in several Failed events, as described below. The Event Properties allow you to get a more specific reason why an event failed.

- **If Folder Monitor Failure reason**—Available only with the Folder Monitor Failed Event.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the Failure reason **does/does not** equal to **[reason]**.
  3. Click the **[reason]**link to specify which sort of failure to trigger on: **any failure**, **archive failed**, or **health check failed**.
- **If Event Reason**—The Event was triggered by one of the reasons in the table below. Available reasons depend on the Event trigger (**User Connect Failed**, **User Login Failed**, **User Logged Out**, **Download Failed**, **Upload Failed**, **Verified Upload Failed**, **Verified Download Failed**). For example, **IP address was rejected** can apply to the **User Connect Failed** Event; but cannot apply to any other Event triggers.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the Event Reason **does/does not** equal to **[specific reason]**.



  3. Click the **[specific reason]** link to specify which sort of failure to trigger on (refer to table below for Event Reasons).

	Connection Event	User Events		File Server Events			
Event Reason	**User Connect Failed**	**User Login Failed**	**User Logged Out**	**Download Failed**	**Upload Failed**	**Verified Upload Failed**	**Verified Download Failed**
Aborted by user				X	X	X	X
Access denied				X	X	X	X
Account Disabled		X					

	Connection Event	User Events		File Server Events			
Event Reason	**User Connect Failed**	**User Login Failed**	**User Logged Out**	**Download Failed**	**Upload Failed**	**Verified Upload Failed**	**Verified Download Failed**
Account Locked Out (v6.1 and later)		X					
Client SSL Certificate was rejected	X						
Connection closed				X	X	X	X
File is banned				X	X	X	X
File not found				X			
FTP Session was closed because of error			X				
FTP Session was closed by timeout			X				
FTP Session was closed by user (QUIT)			X				
Invalid password		X					
IP address was banned			X				
IP address was rejected	X						
IP address was rejected and banned	X						
Max incorrect password attempts reached			X				
Protocol not supported		X					
Quota exceeded					X	X	X
Restricted IP		X					
TCP/IP connections was closed by peer			X				
Too many connections per IP	X	X					
Too many connections per Site	X	X					

	Connection Event	User Events		File Server Events			
Event Reason	**User Connect Failed**	**User Login Failed**	**User Logged Out**	**Download Failed**	**Upload Failed**	**Verified Upload Failed**	**Verified Download Failed**
Too many connections per user		X					
User was kicked by administrator			X				

Related Topics

- Using Conditions
- Condition Placement
- Changing Condition Placement
- Condition Evaluation
- Else Clauses
- Logical Operators
- Evaluating Expressions
- The Compound Conditional Statement
- Events and Available Variables

Advanced Workflow Conditions

You can apply Advanced Workflow Conditions to any events except the Cloud-Based events.

To use one or more Advanced Workflow Conditions

1. Create the Event Rule.
2. Double-click the Condition, or click the Condition, then click **Add Condition**.
3. In the **Rule Builder**, click the hyperlinks in the Condition to specify if the Condition **does** or **does not** and **less than**, **equal to**, or **greater than** the [code], [test], or [number].
4. Then add one or more Actions and click **Apply**.

> **NOTE:** The Advanced Workflow Conditions below are available for any events except cloud-based events. They are named for their function. For example, the "If Advanced Workflow Error Description" condition will trigger the event if the Error Description in the Advanced Workflow has or doesn't have the text specified.

- If Advanced Workflow Error Code does, does not, less than, equal to, or greater than [code]
- If Advanced Workflow Error Description does, does not, equal to [text]
- If Advanced Workflow Error Line does, does not, less than, equal to, or greater than [number]
- If Advanced Workflow Result Code does, does not, less than, equal to, or greater than [code]
- If Advanced Workflow Result Description does, does not, equal to [text]
- If Advanced Workflow Execution Time does, does not, less than, equal to, or greater than [ms]

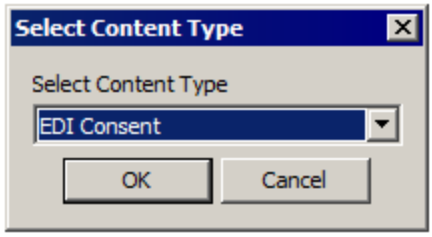
Related Topics

- Adding a Workflow Action to an Event Rule
- Creating Workflows for use in Event Rules

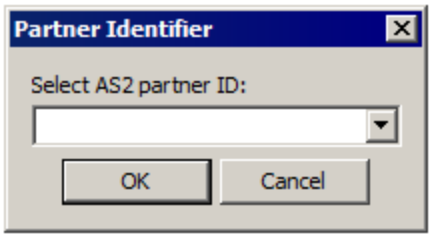
AS2 Conditions

You can apply AS2 Conditions to File Uploaded and AS2-related events.

- **If AS2 Content Type**. Tests whether the AS2 content matches the specified content type.
  1. Add the Condition to a Rule.
  2. In the Rule Builder, click the linked text to specify whether the content type **does/does not** equal to **[specific AS2 content type]**. Click **[specific AS2 content type]** to open the **Select Content Type** dialog box.



  3. Click the **Select Content Type** drop-down list to specify a (**X12**, **EDIFACT**, **XML**, **EDIConsent**, **Binary**, **Plaintext**).
  4. Click **OK**.
- **If AS2 Partner ID**. Tests whether the AS2 Partner ID matches the specified mask.
  1. Add the Condition to a Rule.
  2. In the Rule Builder, click the linked text to specify whether the partner ID **does/does no**t equal to **[specific AS2 Partner ID]**. Click **[specific AS2 Partner ID]** to open the **Partner Identifier** dialog box.



  3. Click the **Select AS2 partner ID** drop-down list to specify a partner.
  4. Click **OK**.

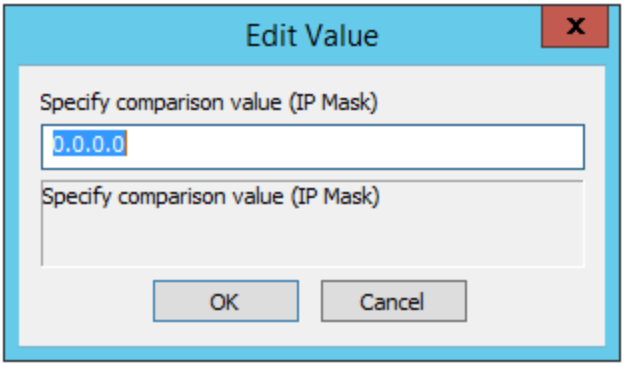
You can also specify the AS2 protocol with the **If Protocol Condition** described in Connection Conditions.

Connection Conditions

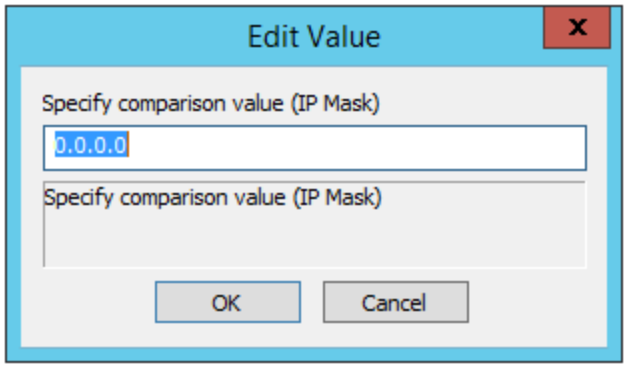
You can apply these Conditions to Connection Events, File system Events, and certain User Events.

By default, IP Access-related Event Rules are limited to 1000 rules.

- **If Remote IP**—a connection is made from a remote IP address that matches/does not match an IP address or IP mask.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the remote IP address **does** or **does not** match **[ip mask]**.
  3. Click **[ip mask]** to open the **Edit Value** dialog box.

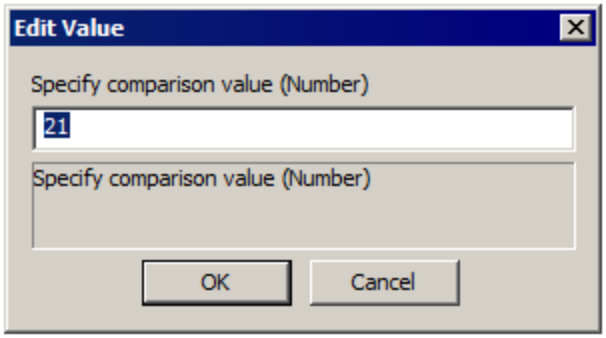


  4. Specify an IP address or and/or wildcards, and then click **OK** to add the Condition to the Event trigger.
- **If Local IP**—a connection is made to a local IP address that matches/does not match an IP address or IP mask.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the local IP address **does** or **does not** match **[ip mask]**.
  3. Click **[ip mask]** to open the **Edit Value** dialog box.

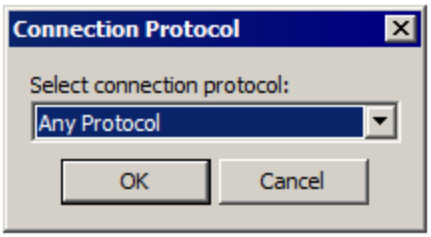


4. Specify an IP address or and/or wildcards, and then click **OK** to add the Condition to the Event trigger.

- **If Local Port**—a connection is made/not made on a port/range of ports.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the port number **does/does not equal to, greater than or equal to, less than, less than or equal to [value]**.
  3. Click [value] to open the **Edit Value** dialog box.



  4. Specify a port number, and then click **OK** to add the Condition to the Event trigger.
- **If Protocol**—Trigger the Rule when a specific protocol is used or not used.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the protocol **does/does not equal to [ftp/ssl/tls/sftp/http/https/as2/adhoc]**.
  3. Click **[ftp/ssl/tls/sftp/http/https/as2/adhoc]** to open the **Connection Protocol** dialog box.



4. Click the **Select connection protocol** drop-down list to select the protocol (or specify **Any Protocol**).
5. Click **OK**.

- **If HTTP Query String**—does/does not contain/equal to <string>. Specify a string; enclosing quotes are not needed
- **If HTTP Headers List**—does/does not contain/equal to <string>. Specify a string; enclosing quotes are not needed

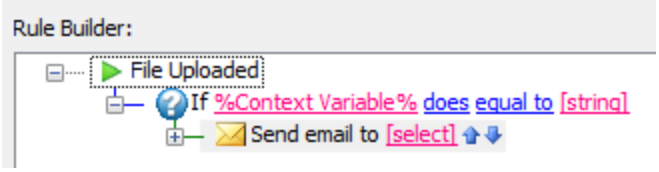
Context Variable Condition

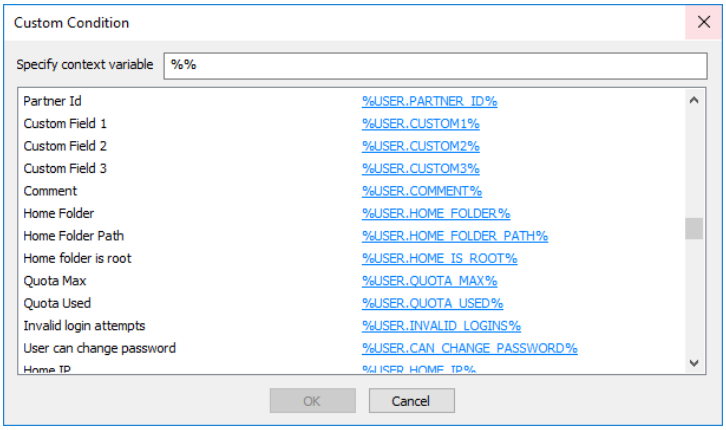
The Context Variable Condition is triggered when a context variable meets specific criteria: if %Context_Variable% is/is not, does/does not, equal/less than/greater than/, contain/start with a specified value. For example, %USER.HOME_FOLDER_PATH% to provide entire path to a user's home folder (for example, C:\InetPub\EFTRoot\MySite\Usr\asmith).

(This is an oversimplified example; putting this Rule on a production network could potentially create huge logs.)

To use the Context Variable Conditions

1. Create an Event Rule and add one or more actions.
2. Add the **Context Variable** Condition.





File System Conditions

You can apply File System Conditions only to File system Events and the Folder Monitor Event.

- If Base File Name
- If Destination File Name
- If File Change
- If File (or Folder) does exist at [path]
- If File Name
- If File Size
- If Physical Destination Folder Name
- If Physical Destination Path
- If Physical Folder Name
- If Physical Path
- If Virtual Destination Path
- If Virtual Directory Name
- If Virtual Folder Name
- If Virtual Path

Using the File System Conditions

- **If File (or Folder) does exist at [path]**—a file or folder does or does not exist at specified path or variable.

- **If File Change**—a file is/is not added, removed, or renamed in a folder. This Condition is added automatically when you create a **Folder Monitor** Event.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the file change **does/does not** equal to **added**, **removed**, or **renamed**.
- **If Virtual Path**—the file or folder exists, does not exist at a virtual location and/or wildcard.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
  3. Click **[path mask]**to open the **Choose Virtual Path**dialog box.

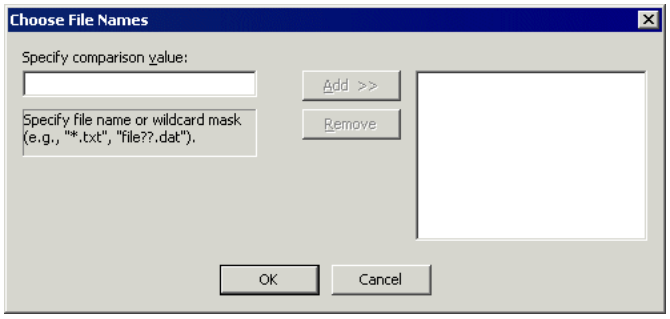
4. Specify a path or wildcard, then click **Add**to move the path to the right text box.
5. To remove a path, in the right text box, click the path or wildcard, and then click **Remove**.
6. Click **OK**to add the Condition to the Event trigger.

- **If Physical Path**—the file or folder exists, does not exist at a physical location (the full folder path including the file name or wildcard).
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
  3. Click **[path mask]**to open the **Choose Physical Paths**dialog box.
  4. Specify a path or wildcard, then click **Add**to move the path to the right text box. You can add multiple paths.
  5. To remove a path or wildcard, in the right text box, click the path or wildcard, and then click **Remove**.
  6. Click **OK**to add the Condition to the Event trigger.
- **If Virtual Directory Name**—the virtual directory name does or does not match the path mask.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual directory name **does/does not match [path mask]**.
  3. Click **[path mask]** to open the **Choose Virtual Directory Names** dialog box.
  4. Specify a folder name or wildcard, and then click **Add** to move the folder name or wildcard to the right text box. You can add multiple folders.
  5. To remove a folder name or wildcard, in the right text box, click the folder name or wildcard, and then click **Remove**.
  6. Click **OK**to add the Condition to the Event trigger.
- **If Physical Folder Name**—the file or folder exists, does not exist in a physical folder (the folder path or wildcard without a file name).
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
  3. Click **[path mask]**to open the **Choose Folder Names**dialog box.
  4. Specify a folder name or wildcard, then click **Add** to move the folder name or wildcard to the right text box. You can add multiple folders.
  5. To remove a folder name or wildcard, in the right text box, click the folder

name or wildcard, and then click **Remove**.

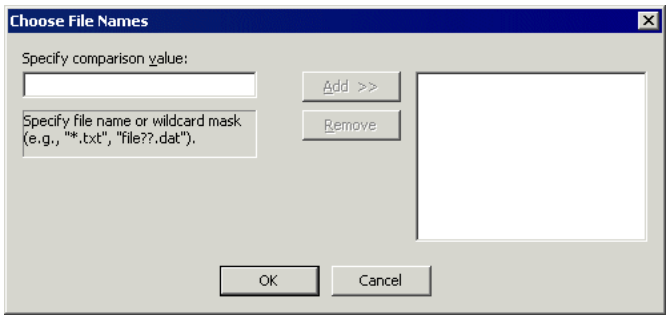
6. Click **OK**to add the Condition to the Event trigger.

- **If Virtual Folder Name**—the file or folder exists, does not exist in a virtual folder.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual folder name **does/does not match/start with [path mask]**.
  3. Click **[path mask]**to open the **Choose Virtual Folder Names** dialog box.
  4. Specify a folder name or wildcard, and then click **Add** to move the folder name or wildcard to the right text box. You can add multiple folders.
  5. To remove a folder name or wildcard, in the right text box, click the folder name or wildcard, and then click **Remove**.
  6. Click **OK**to add the Condition to the Event trigger.
- **If File Name**—the file name matches/does not match a string of characters and/or wildcard.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does not** match **[path mask]**.
  3. Click **[path mask]**to open the **Choose File Names**dialog box.



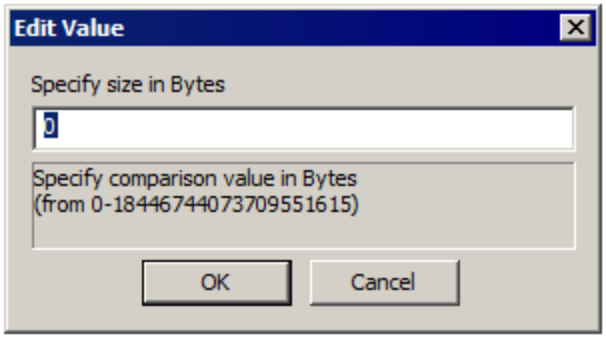
  4. Specify a file name or wildcard, then click **Add** to move the file name or wildcard to the right text box. You can add multiple file names.
  5. To remove a path, in the right text box, click the file name or wildcard, and then click **Remove**.
  6. Click **OK**to add the Condition to the Event trigger.
- **If Base File Name**—The portion of the filename to the left of the right most period; provided as a way to support rename. For example, if a file is downloaded as SomeFile.ext.tmp, the Base File Name is: SomeFile.ext.

1. Add the Condition to the Event Rule.
2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does not** match **[mask]**.
3. Click **[mask]**to open the **Choose File Names**dialog box.



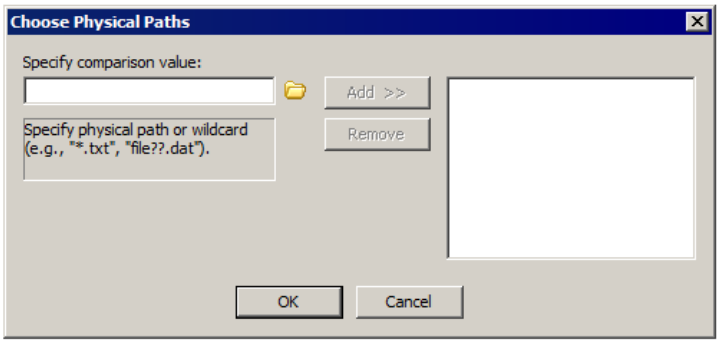
4. Specify a file name or wildcard, then click **Add** to move the file name or wildcard to the right text box. You can add multiple file names.
5. To remove a file name or wildcard, in the right text box, click the file name or wildcard, and then click **Remove**.
6. Click **OK**to add the Condition to the Event trigger.

- **If File Size**—the file size is or is not less than, equal to, or greater than a specified number of bytes.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the file size **is/is not equal to, greater than or equal to, less than, less than or equal to [size (B)]**. Click **[size (B)]** to open the **Edit Value** dialog box.



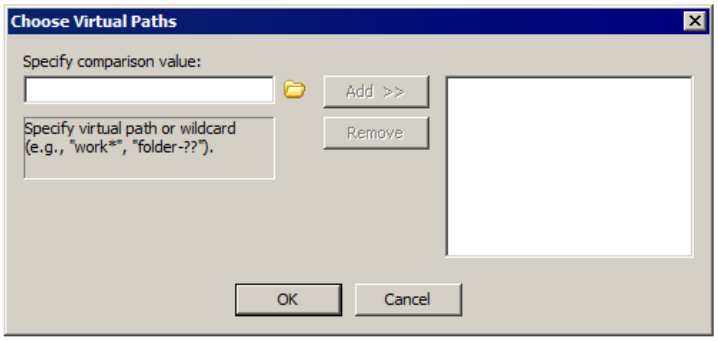
  3. Specify a file size in bytes, and then click **OK**.
- **If Physical Destination Path**—(for **File Moved** Event) the file or folder exists, does not exist at a physical location and/or wildcard.

1. Add the Condition to the Event Rule.
2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
3. Click **[path mask]**to open the **Choose Physical Paths**dialog box.



4. Specify a path or wildcard, then click **Add**to move the path or wildcard to the right text box. You can add multiple paths.
5. To remove a path or wildcard, in the right text box, click the path or wildcard, and then click **Remove**.
6. Click **OK**to add the Condition to the Event trigger.

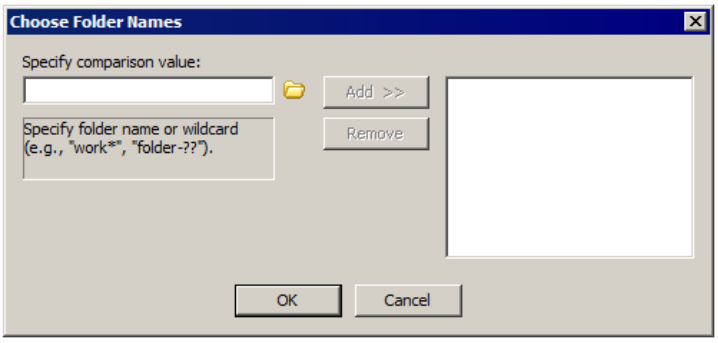
- **If Virtual Destination Path**—(for **File Moved** Event) the file or folder exists, does not exist at a virtual location (the full folder path including the file name and/or wildcard).
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
  3. Click **[path mask]**to open the **Choose Virtual Paths**dialog box.



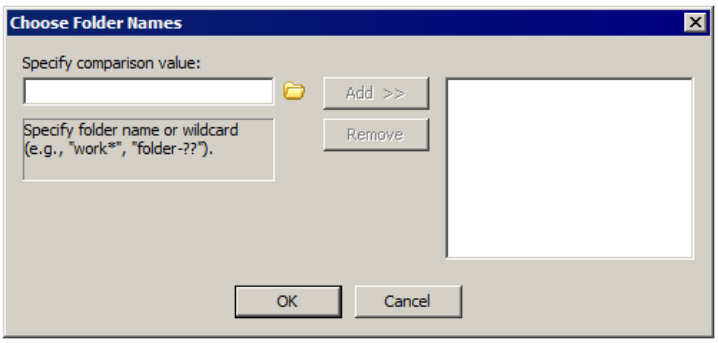
  4. Specify a path or wildcard, then click **Add**to move the path to the right text box. You can add multiple paths.

5. To remove a path or wildcard, in the right text box, click the path or wildcard, and then click **Remove**.
6. Click **OK**to add the Condition to the Event trigger.

- **If Physical Destination Folder Name**—(for **File Moved** Event) the physical folder name matches/does not match a physical folder name and/or wildcard.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does notmatch/start with[path mask]**.
  3. Click **[path mask]**to open the **Choose Folder Names**dialog box.



  4. Specify a folder name or wildcard, then click **Add** to move the folder name or wildcard to the right text box. You can add multiple names.
  5. To remove a folder name or wildcard, in the right text box, click the folder name or wildcard, and then click **Remove**.
  6. Click **OK**to add the Condition to the Event trigger.
- **If Destination File Name**—(for **File Moved** Event) the destination file name matches/does not match a string of characters and/or wildcard.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does not** match **[path mask]**.
  3. Click **[path mask]**to open the **Choose File Names**dialog box.



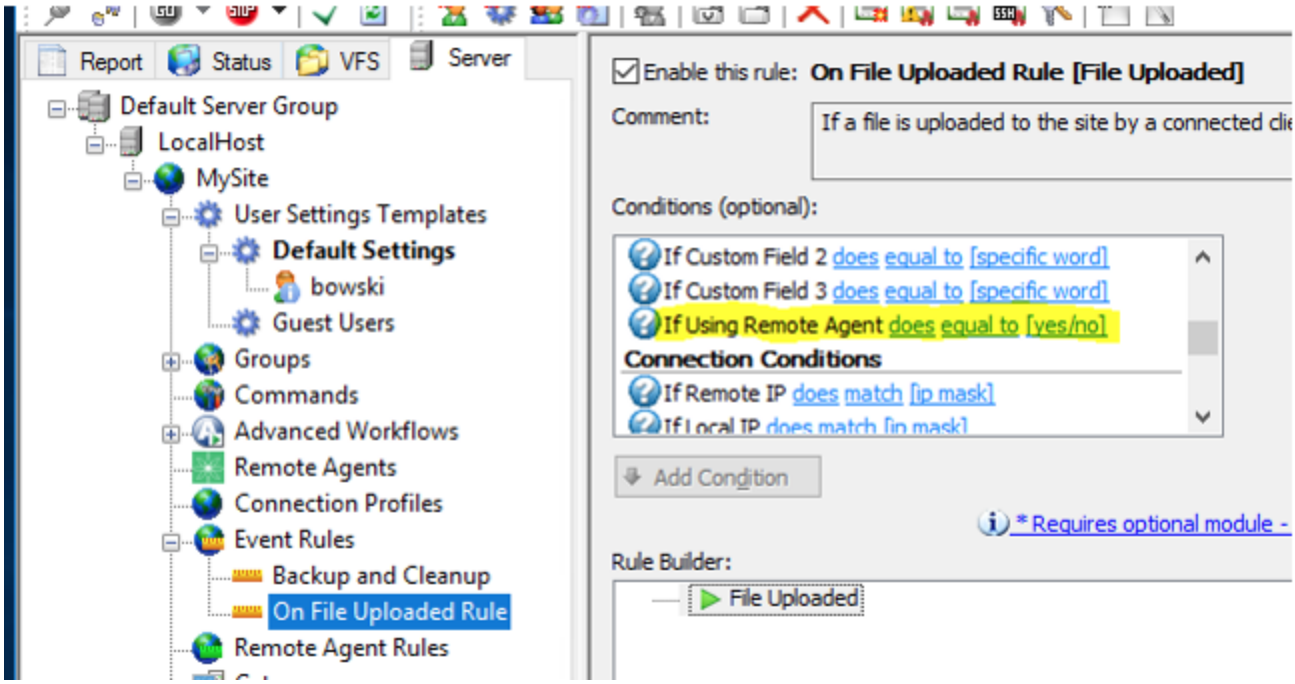
4. Specify a file name or wildcard, then click **Add** to move the file name or wildcard to the right text box. You can add multiple names.
5. To remove a file name or wildcard, in the right text box, click the file name or wildcard, and then click **Remove**.
6. Click **OK**to add the Condition to the Event trigger.

Remote Agent Event Rule Conditions

You can add a "If using Remote Agent does/does not equal to yes/no" to EFT Event Rules for the following events:

- File Uploaded
- File Downloaded
- File Upload Failed
- File Download Failed
- Before Download

This Condition works for HTTP and HTTPS interactions only.



Secure Message Conditions

Secure Message Conditions are available for Outlook Add-In, Send Portal, Reply, Drop Off, and Request File-related events.

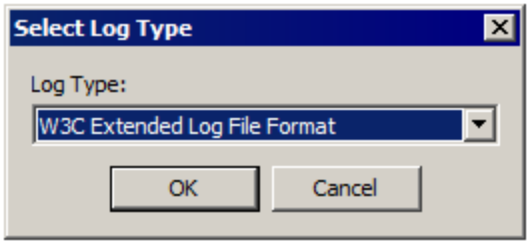
To use these conditions, add a Condition to the Rule, then click the linked text to specify the parameters. For each Condition, specify that the Condition does or does not equal the specified parameter.

- **If Portal From** does or does not equal to [specific portal type] - Specify a portal type: OAI, Send Portal, Reply, Drop Off, or Request File.
- **If Sender** does or does not equal to [text] - Specify a sender in the text box.
- **If Send Error** does or does not equal to [text] - Specify a send error in the text box.
- **If Subject** does or does not equal to [text] - Specify a subject in the text box.
- **If To Recipients** does or does not equal to [specified name(s)] - Specify a recipient in the string box.
- **If CC Recipients** does or does not equal to [specified name(s)] - Specify a recipient in the string box.
- **If BCC Recipients** does or does not equal to [specified name(s)] - Specify a recipient in the string box.
- **If Attachments** does or does not equal to [specified name(s)] - Specify a name in the string box.
- **If Attachments Storage Path** does or does not equal to [path mask] - Specify a value in the box.
- **If Body** does or does not equal to [text] - Specify a string for comparison.
- **If Body Is Secured** does or does not equal to [yes/no] - Click to specify yes or no.
- **If Message Is Single Use** does or does not equal to [yes/no] - Click to specify yes or no.
- **If Message Requires Account to Reply** does or does not equal to [yes/no] - Click to specify yes or no.
- **If Message Requires Account to View** does or does not equal to [yes/no] - Click to specify yes or no.
- **If Message Expires On** does or does not equal to [specific timestamp] - Specify a string to match a timestamp.
- **If Notification Frequency**does or does not equal to [specific type] - Specify the notification frequency, IMMEDIATE, DAILY, NEVER.

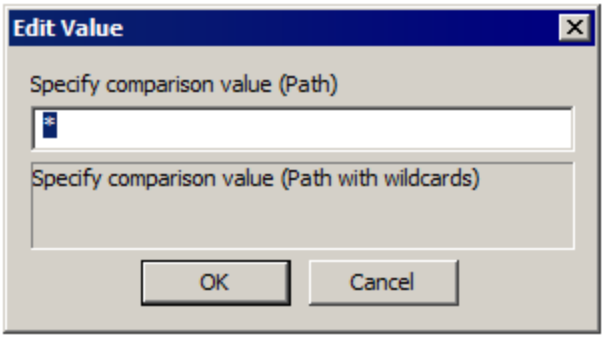
Server Conditions

You can apply Server Conditions to certain Server Events, Operating System Events, File Server Events, and the **IP Added to Ban List**SiteEvent.

- **If Server Running**—The EFT service is currently running.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the Server **does/does not** equal to **Yes/No**.
- **If Log Type**—The log type is/is not a specific type.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the log type **does/does not** equal to **[specific type]**.
  3. Click **[specific type]** to open the **Select Log Type** dialog box.

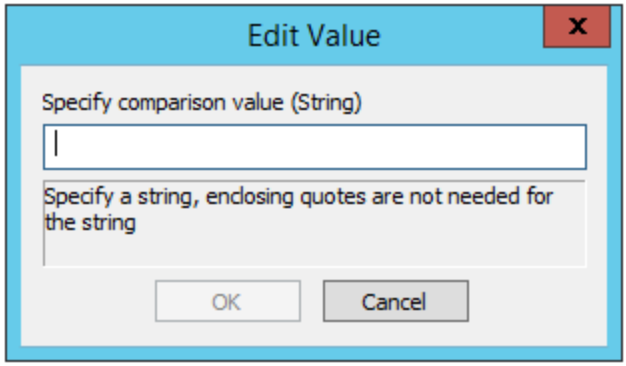


  4. Specify a **Log Type**, and then click **OK**.
- **If Log Location**—The log location matches a specific path.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the log location **does/does not** match **[path]**.
  3. Click **[path]**to open the **Edit Value**dialog box.

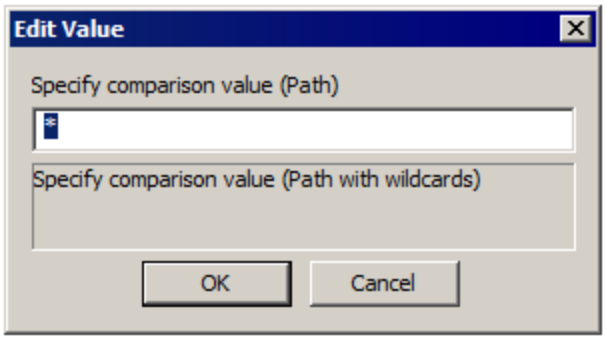


  4. Specify a path or wildcard, and then click **OK**.

- **If Node Name**—In HA cluster, EFT name matches/does not match a specific character string. Most often used when you want only one specific node to send email notifications or perform other actions. Not specifying a node can cause multiple nodes to perform the Action specified in the Event Rule.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the node name **does/does not** equal to **[name]**.
  3. Click **[name]**to open the **Edit Value**dialog box.

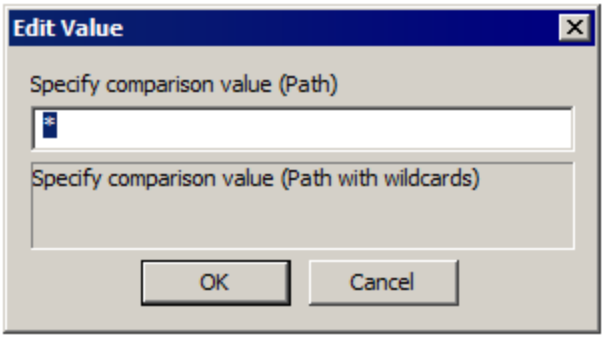


  4. Specify a name or wildcard, and then click **OK**.
- **If Old Log File Path**—(Used with the **Log Rotated** Event only) The old log file path matches a specific path.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the old log location **does/does not** match **[path]**.
  3. Click **[path]**to open the **Edit Value**dialog box.

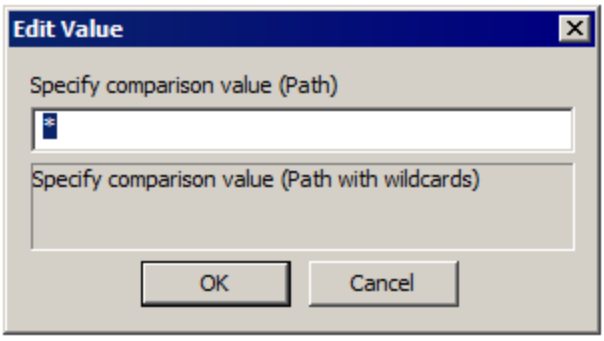


  4. Specify a path or wildcard, and then click **OK**.

- **If New Log File Path**—(Used with the **Log Rotated** Event only) The new log file path matches a specific path.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the new log location **does/does not** match **[path]**.
  3. Click **[path]**to open the **Edit Value**dialog box.

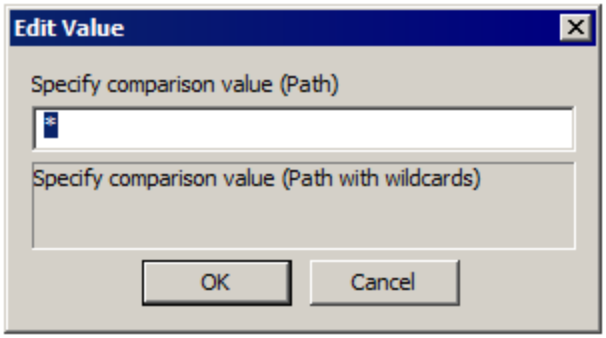


  4. Specify a path or wildcard, and then click **OK**.
- **If Old Log File Name**—(Used with the **Log Rotated** Event only) The old log file name matches a specific name.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the old log location **does/does not** match **[path]**.
  3. Click **[path]**to open the **Edit Value**dialog box.



  4. Specify a path or wildcard, and then click **OK**.

- **If New Log File Name**—(Used with the **Log Rotated** Event only) The new log file name matches a specific name.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the new log location **does/does not** match **[path]**.
  3. Click **[path]**to open the **Edit Value**dialog box.



  4. Specify a path or wildcard, and then click **OK**.

Site Conditions

You can apply the Site Condition only to these User events: **User Account Disabled**, **User Password Changed**, **User Account Created** Events.

- **If Site running**—The Site is started or stopped.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the Site Running **does/does not** equal to **yes/no**.

User Conditions

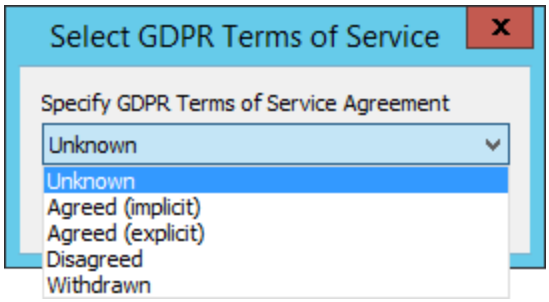
You can apply User Conditions to User Events and File system Events.

- In each of the GDPR-specific user conditions, click an option, then click **OK**.

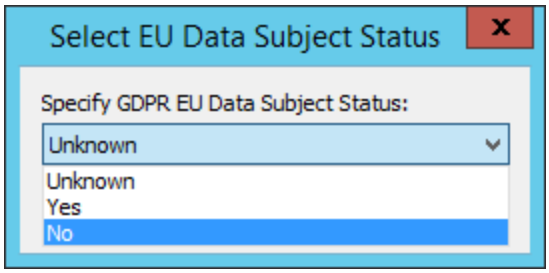
  For example, suppose you want to be notified any time an EU Data Subject joins a Workspace. You could configure an Event Rule to trigger on the **User Joins Workspace** event, with the **EU data Subject Status** condition set to **Yes**, and a **Send email notification**Action (with applicable content variables added), which could send that information to your email or the Data Protection Officer's email.

  - **If (GDPR) User consent to privacy policy** does or does not equal to:

  - **If (GDPR) User agreement to terms of service** does or does not equal to:

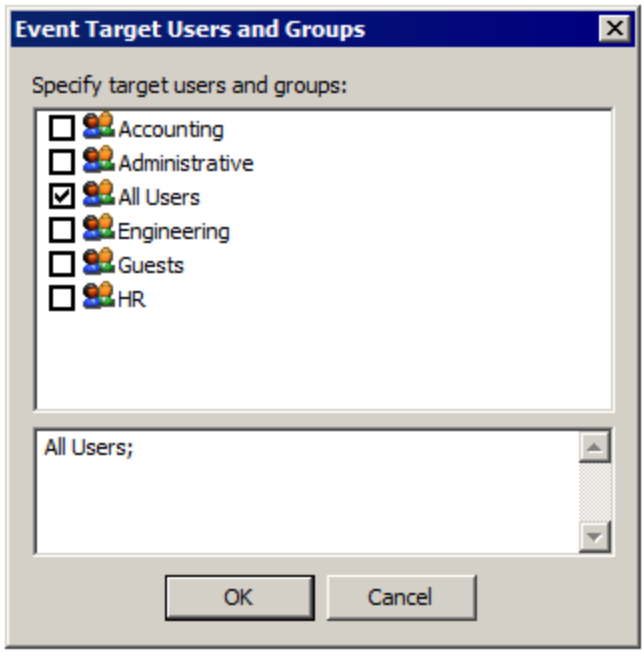


  - **If (GDPR) User EU data subject status** does or does not equal to:

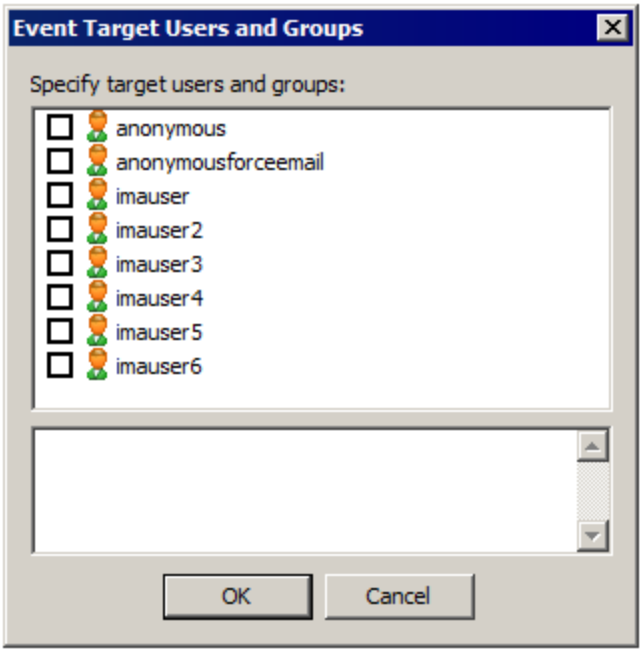


- **If DUNS number** does or does not equal to [specific word]. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If (GDPR) Right exercised article** ID does or does not equal [specific article ID]
- **If (GDPR) Reason given** does or does not equal to [specific word or phrase]. In the **Edit Value** dialog box, specify a string, and then click **OK**.

- **If User**—the user account is or not a member of one or more Groups.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the user group **is/is not** a member of **[specific group(s)]**.
  3. Click **[specific group(s)]** to open the **Event Target Users and Groups** dialog box.

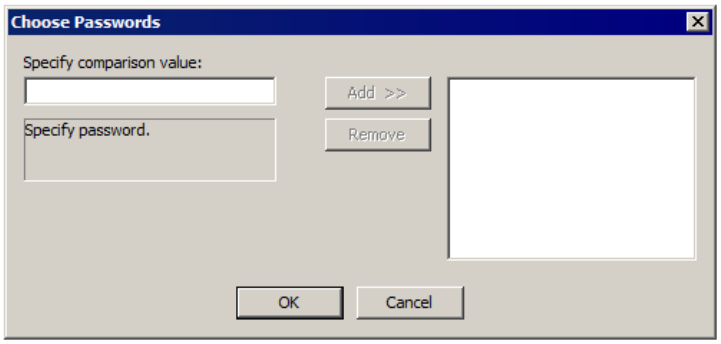


  4. Select the check box of the users/groups that will trigger the Event and clear the **All Users** check box if you don't want the Condition to apply to all users.
  5. Click **OK**to add the Condition to the Event trigger.
- **If Logon Name**—the user's username matches/does not match a specific username.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the logon name **is/is not** one of **[specified name(s)]**.
  3. Click **[specified name(s)]** to open the **Event Target Users and Groups** dialog box.



4. Select the check box of the users/groups that will trigger the Event and clear the **All Users** check box if you don't want the Condition to apply to all users.
5. Click **OK**to add the Condition to the Event trigger.

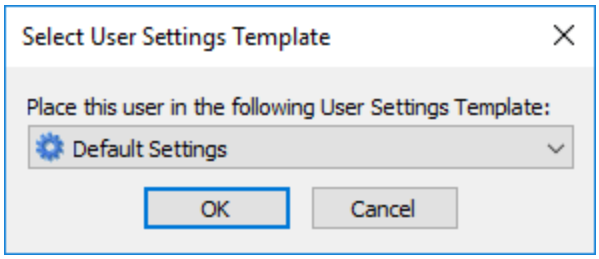
- **If Logon Password**—the user's password matches/does not match a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the logon password **is/is not** one of **[specified password(s)]**.
  3. Click **[specified password(s)]** to open the **Choose Passwords** dialog box.



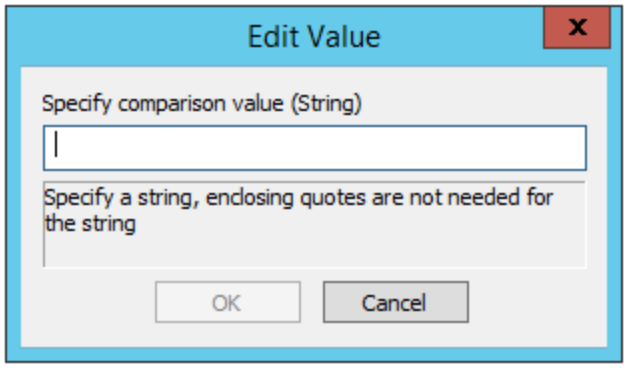
  4. Specify a password, and then click **Add**to move the password to the right text box.

5. To remove a password, in the right text box, click the password, and then click **Remove**.
6. Click **OK**to add the Condition to the Event trigger.

- **If Account Enabled**—the user account is enable or not enabled
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the account **does/does not** equal to **Yes/No**.
- **If Settings Template**—the user belongs/does not belong to a Settings Template.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the Settings Template **does/does not** equal to **[Settings Template]**.
  3. Click **[Settings Template]** to open the **Select Settings Template** dialog box.

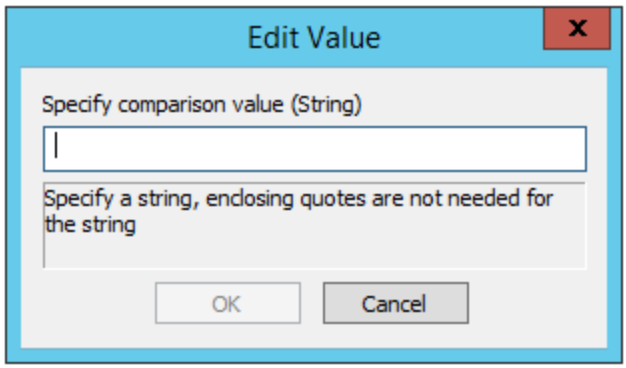


  4. Specify a Settings Template, then click **OK**. (Even if there is only one Settings Template, you still have to click **OK**in the **Select Settings Template**dialog box to complete the Condition.)
- **If Full Name**—a user's name matches/does not match, contains/equals a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the user account name **does/does not equal to/contain [specific word]**.
  3. Click **[name]**to open the **Edit Value**dialog box.



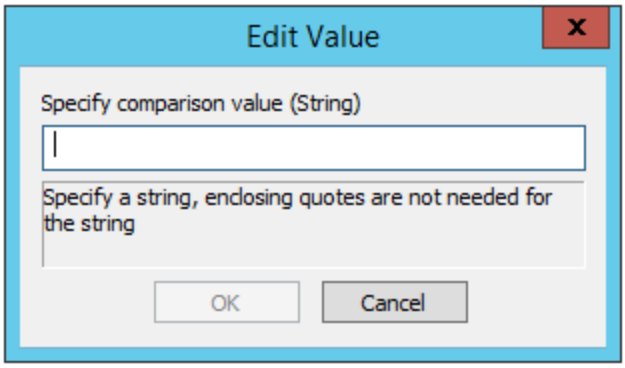
4. In the **Edit Value**dialog box, specify a string, and then click **OK**.

- **If Description**—the user's description matches/does not match, contains/equals a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the description **does/does not equal to/contain [specific word]**.
  3. Click **[name]**to open the **Edit Value**dialog box.



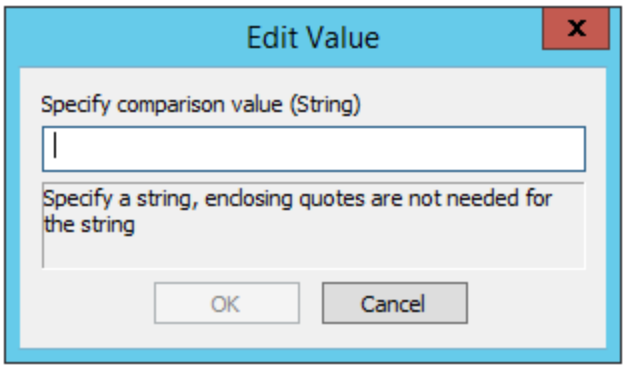
4. In the **Edit Value**dialog box, specify a word, and then click **OK**.

- **If Comment**—the user's comment matches/does not match, contains/equals a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the comment **does/does not equal to/contain [specific word]**.
  3. Click **[name]**to open the **Edit Value**dialog box.

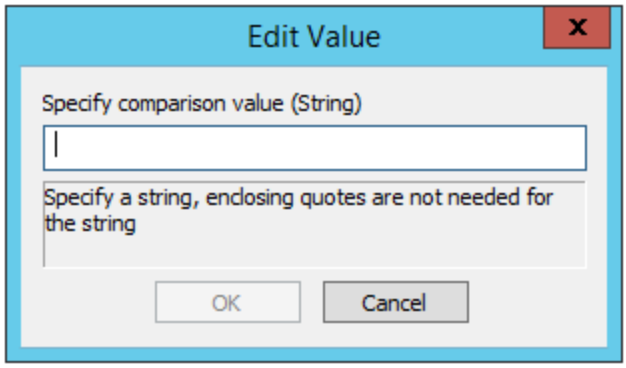


4. In the **Edit Value**dialog box, specify a string, and then click **OK**.

- **If EMail Address**—the user's email address matches/does not match, contains/equals a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the email address **does/does notequal to/contain[specific word]**.
  3. Click **[name]**to open the **Edit Value**dialog box.

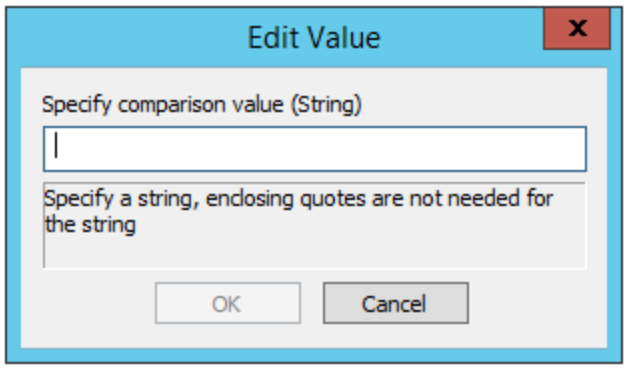


  4. In the **Edit Value**dialog box, specify a string, and then click **OK**.
- **If Phone Number**—the user's phone number matches/does not match, contains/equals a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the phone number **does/does not equal to/contain [specific word]**.
  3. Click **[name]**to open the **Edit Value**dialog box.

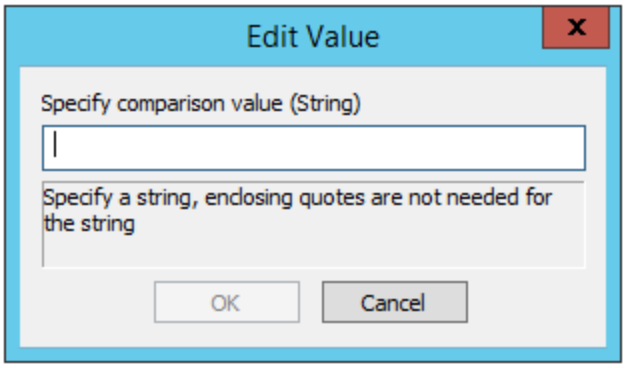


4. In the **Edit Value**dialog box, specify a string, and then click **OK**.

- **If Pager Number**—the user's pager number matches/does not match, contains/equals a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the pager number **does/does not equal to/contain [specific word]**.
  3. Click **[name]**to open the **Edit Value**dialog box.

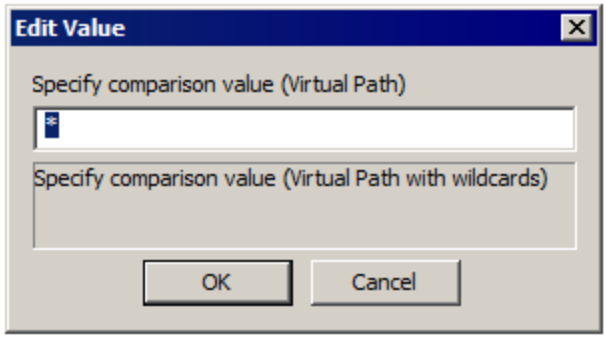


  4. In the **Edit Value**dialog box, specify a string, and then click **OK**.
- **If Fax Number**—the user's fax number matches/does not match, contains/equals a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the fax number **does/does not equal to/contain [specific word]**.
  3. Click **[name]**to open the **Edit Value**dialog box.

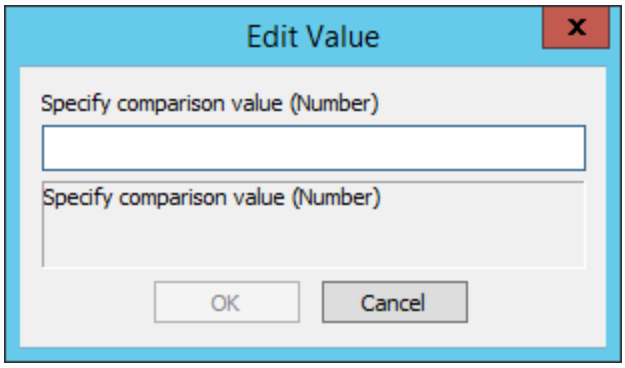


4. In the **Edit Value**dialog box, specify a string, and then click **OK**.

- **If Home Folder**—the location of a user's home folder matches/does not match a physical location.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the home folder **does/does not** match **[path]**.
  3. Click **[path]**to open the **Edit Value**dialog box.

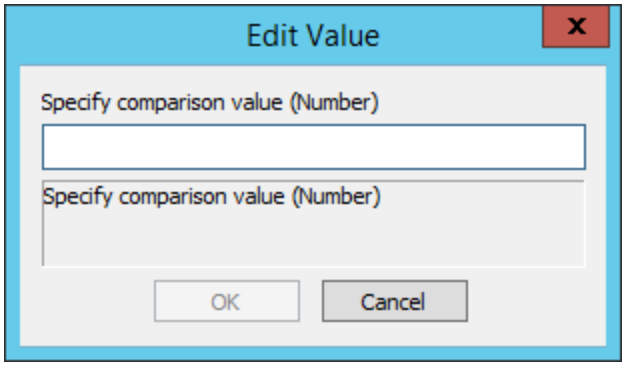


  4. Specify a virtual path, and then click **OK**.
- **If Home Folder is root**—the user's home folder is/is not their root directory.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether home folder root **does/does not** equal to **[yes/no]**.
- **If Quota Max**—the user's account has a size limit **less than/equal to/not less than/not equal** to a size in megabytes.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the maximum quota **does/does not** equal to **[size (MB)]**.
  3. Click **[size (MB)]** to open the **Edit Value** dialog box.

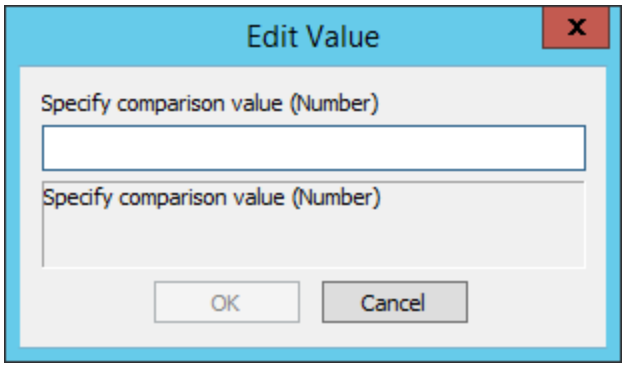


4. Specify the maximum quota, and then click **OK**.

- **If Quota Used**—the user's filled disk space is/is not less than/equal to/greater than an amount of allowed disk space.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the home folder **is/is not equal to, greater than or equal to, less than, less than or equal to [size (MB)]**.
  3. Click **[size (MB)]** to open the **Edit Value** dialog box.



  4. In the **Edit Value**dialog box, specify a value, and then click **OK**.
- **If Invalid login attempts**—the user's failed login attempts are/are not less than, equal to, greater than a number.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether invalid login attempts **is/is not equal to, greater than or equal to, less than, less than or equal to [number]**.
  3. Click **[number]** to open the **Edit Value** dialog box.

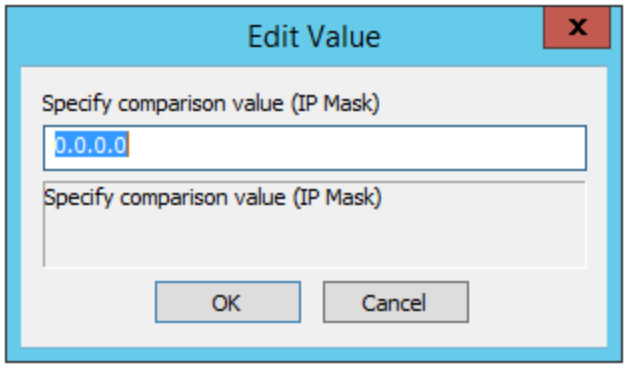


4. In the **Edit Value**dialog box, specify a string, and then click **OK**.

- **If User can change password**—the user has/does not have permission to change the login password.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether user can change password **does/does not** equal to **[yes/no]**.
- **If Home IP**—the user's allowed IP address matches/does not match an IP address or set of IP addresses.

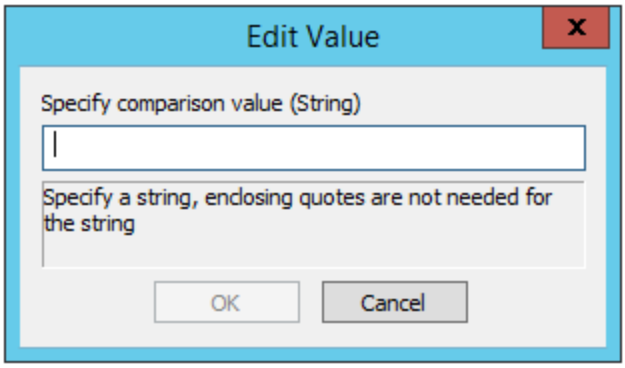
  By default, IP Access-related Event Rules are limited to 1000 rules.

  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the home IP **does/does not** match **[ip mask]**.
  3. Click **[ip mask]**to open the **Edit Value**dialog box.



  4. In the **Edit Value**dialog box, specify a string, and then click **OK**.

- **If User can connect using SSL**—the user has/does not have SSL enabled.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether user can connect using SSL **does/does not** equal to **[yes/no]**.
- **If User can connect using FTP**—the user has/does not have FTP enabled.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether user can connect using FTP **does/does not** equal to **[yes/no]**.
- **If User can connect using SFTP**—the user has/does not have SFTP enabled.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether user can connect using SFTP **does/does not** equal to **[yes/no]**.
- **If Account Locked Out**—the user is or is not locked out
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify **does/does not**equal to **[yes/no]**.
- **If Partner Id**- trigger the rule based on the user's Partner ID
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify that the Partner ID **does/does not/ is equal to/ less than/ less than or equal to/ greater than/ greater than or equal to [specific word]**.
- **If Custom Field [1/2/3]**—if user account has information in Custom Field 1, 2, or 3
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the Custom Field **does/does not equal/contain [string]**.
  3. Click linked text to open the **Edit Value** dialog box.

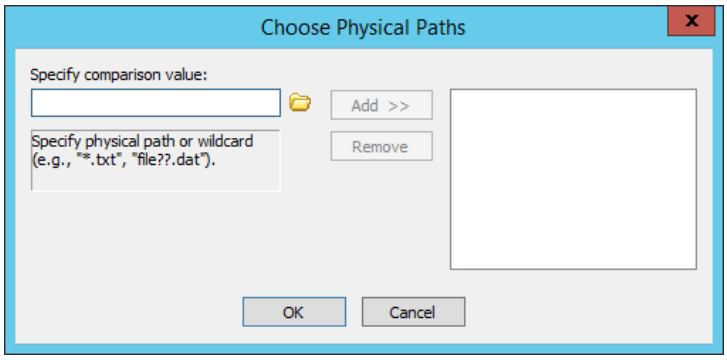


4. In the **Edit Value**dialog box, specify a string, and then click **OK**.

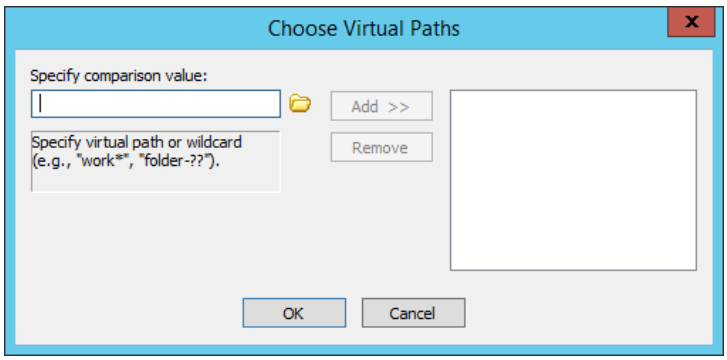
Workspaces Conditions

You can apply these Conditions to File Uploaded events.

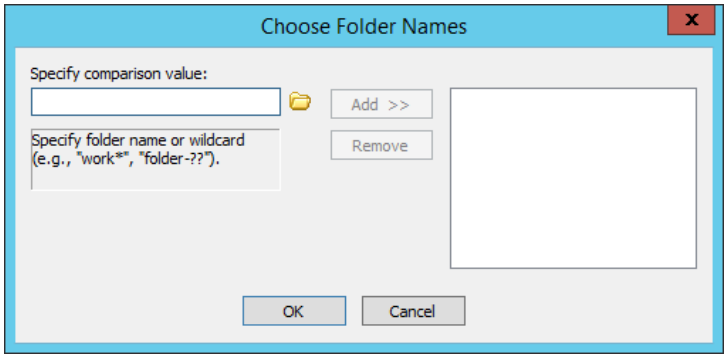
- **If Workspace Physical Path** - Tests whether the physical path does or does not match a path mask. Wildcards can be used.



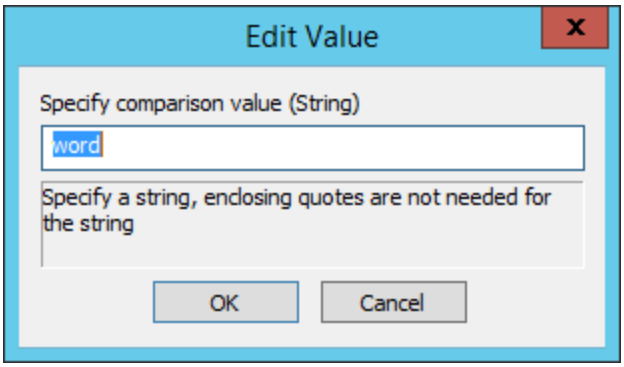
- **If Workspace Virtual Path** - Tests whether the virtual path does or does not match a path mask. Wildcards can be used.



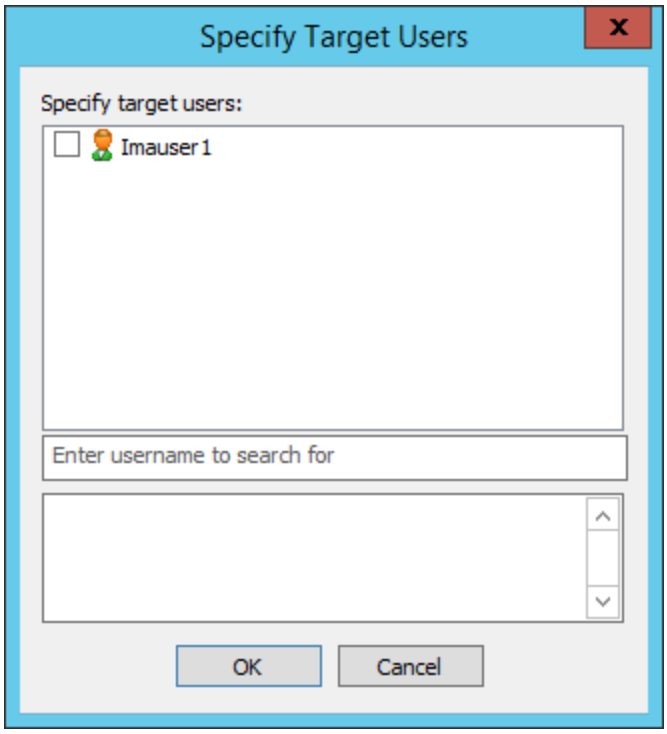
- **If Workspace Name** - Tests whether the folder name does or does not match a mask. Wildcards can be used.



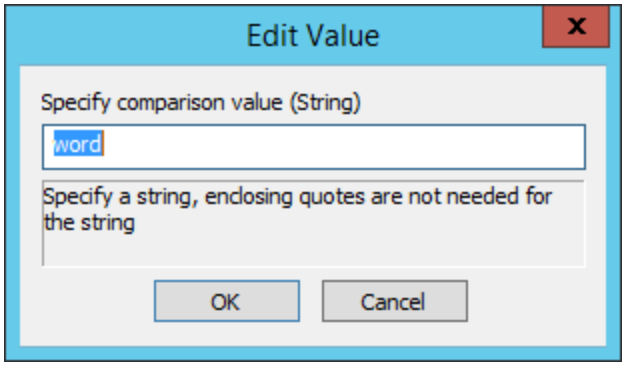
- **If Workspace Participants List** - Tests whether the participant list does or does not contain a string specified.



- **If Workspace Owner** - Tests whether the Workspace Owner is or is not one of a list of specified users.



- **If Workspace Owner Email Address** - Tests whether the Workspaces Owner email address does or does not contain or is equal to a specified string.



Auditing and Reporting Module

The topics below provide the procedures for configuring and using Auditing and Reporting with EFT. (Requires ARM license)

- Introduction to Auditing and Reporting
- Installing and Configuring the Auditing and Reporting
- Activating the Auditing and Reporting Module
- Auditing and Reporting Interface
- ARM Database
- Auditing
- Security Auditing
- Reporting

Introduction to the Auditing and Reporting Module

The Auditing and Reporting Module (ARM) captures the transactions passing through EFT and provides an interface where you can use preconfigured reports or create your own custom reports to query, filter, and view transaction data. Data is stored in a relational database and can be analyzed in real time.

The ARM comes with a number of preconfigured reports to help you start analyzing data right away. The built-in reports were designed to respond to the most common data analysis requests.

Related Topics

- Installing and Configuring Auditing and Reporting
- Activating the Auditing and Reporting Module
- Auditing and Reporting Interface
- ARM Database
- Auditing
- Security Auditing
- Reporting

Installing and Configuring Auditing and Reporting

Auditing and Reporting is normally installed and configured when you install EFT. If you did not install it when you installed EFT, you can run the installer again, choose **Modify**, and then select the **Auditing and Reporting**check box. (Leave the **EFT** and **EFT Administrator Interface** check boxes selected; clearing the check boxes will uninstall them.)

- For EFT to connect to any database, the proper drivers need to be installed on the EFT computer. If the right client-side software (driver) is installed on the EFT computer, the Advanced Workflow module can make the database connection string to get to that database.
- EFT uses Microsoft ActiveX Data Objects (ADO) 2.7 or later to handle database communication, which in turn should load the Oracle drivers to handle Oracle implementation details. How and what is connected largely depends upon the connection string. By default, if you do not supply the entire connection string in EFT, the Oracle connection string should look like:

```
Provider=OraOLEDB.Oracle.1; Data Source=(DESCRIPTION =
(ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = {host
value})(PORT = {port})))"

(CONNECT_DATA =(SERVICE_NAME = {database name})));

Persist Security Info=true;PLSQLRSet=1;PwdChgDlg=0;User Id=
{username};Password={password};
```

NOTE: If you are connecting to an Oracle database, refer to Oracle's documentation regarding Oracle system requirements. Be sure to reboot after you install the Oracle Data Access Components (ODAC). You must install both the 32-bit ODAC drivers for the report writer, and the 64-bit ODAC drivers for EFT to work with Oracle. Refer to the System Requirements for EFT for a list of compatible database versions.

Installation and configuration of the module consists of:

1. Running the EFT installer. The Auditing and Reporting module is normally installed and configured when you install EFT. If you did not install it when you installed EFT, you can run the installer again and choose **Modify**. On the **ARM** page of the installer, click **Configure Auditing and Reporting**.(Follow the procedure in Installing EFT, administrator, and Modules.)

   During installation, EFT needs full DB Owner access to the auditing database to set up the schema. During updates or upgrades, EFT needs full DB Owner access to update the schema. Once it is set up, EFT only needs to be able to read, write, and execute stored procedures.

2. Activating the software with a serial number that includes ARM.
3. Enabling EFT to record data.

How does EFT know which TCP/IP port it should use to connect to SQL Server?

When the SQL Server browser service (installed with SQL Server) starts up, it searches the advanced properties for any "named instances" of SQL Server and which TCP ports they're listening on. When a client wants to connect to a named instance, it asks the browser service (on UDP port 1434) on which TCP/IP port is that instance listening. This is how Microsoft implemented support for multiple instances of SQL Server on the same computer. The default instance listens on TCP port 1433. If you have a named instance, the TCP port is dynamically configured.

This is standard SQL Server functionality and doesn't require special port syntax in the EFT connection string or host name. It's all abstracted by the API used, which looks at the host string and figures out whether you're trying to connect to a named instance or a default instance (by determining whether host\instance or just host was specified).

The SQL Server TCP settings are stored in:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\
MSSQL10.<InstanceName>\MSSQLServer\SuperSocketNetLib\TCP\
```

Refer to the following Microsoft topics for more information:

- For details of how to view/change the TCP information in the SQL Server Configuration Manager, refer to the following MSDN article: http://msdn.microsoft.com/en-us/library/ms177440%28SQL.90%29.aspx, "How to: Configure a Server to Listen on a Specific TCP Port (SQL Server Configuration Manager)."
- http://support.microsoft.com/kb/287932, "Configure the Windows Firewall to Allow SQL Server Access"
- http://msdn.microsoft.com/en-us/library/ms175483.aspx, "Connecting to SQL Server over the Internet"
- http://msdn.microsoft.com/en-us/library/ms181087.aspx, "SQL Server Browser Service"

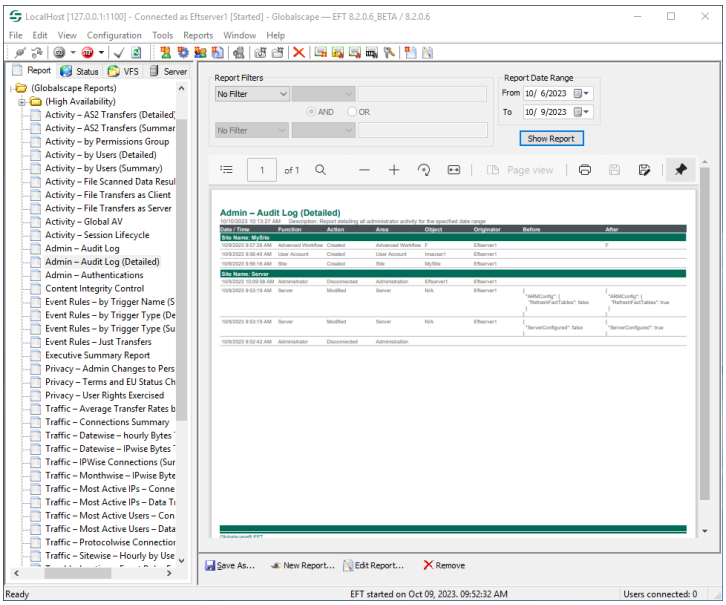
Activating the Auditing and Reporting Module

The Auditing and Reporting Module (ARM) is an add-on to EFT that comes with a unique activation serial number.

- If you have purchased EFT with ARM and have your serial number, follow the normal activation process.
- If you are upgrading, follow the upgradeprocess.

Auditing and Reporting Interface

The **Report** tab of the administration interface is the interface for Auditing and Reporting.



- When you click the **Report**tab in the left pane, the right pane displays the report.
- Using the controls in the right pane, you can view, edit, print, save, and search the report or create a new report.
- You can search for words in the report using the magnifying glass icon.

  The plus and minus and plus icons allow you to zoom in and out
- The rotate icon can change the display from landscape to portrait view.
- The fit-to-width icon is used to fit the page to the window
- When you define a new report template, it appears in the **Custom Reports** node of the tree.
- Refer to Generating a Report, Managing Reports, and Custom Reports for details of running, managing, and defining reports.
- Refer to Descriptions of Preconfigured Reports for descriptions of the report templates in the Globalscape Reports node of the tree.

ARM Database

EFT installs SQL Server Express for test purposes. It is recommended that for production you connect to a SQL Server or Oracle database.

The topics below provide the procedures for managing the ARM database.

- EFT Database Utility
- EFT DB Files
- Database User Account Privileges
- ARM Database Maintenance
- Upgrading the EFT Database
- Upgrading Large Databases
- Manually Creating the ARM Database in SQL Server
- Manually Creating the ARM Database in Oracle

EFT Database Utility

A command line utility is included in the installer that is capable of performing various database-related tasks. This same utility is used by the EFT installer to handle upgrades of existing databases. Typically, all common database tasks are handled by the EFT installer. However, on occasion it may be useful to use the command-line utility to verify the status of a database or perform an upgrade independent of the EFT installation process.

The database utility (DBUtility.exe) is included as part of the core EFT installation. Once installed it is located in the "DBUtility" sub-directory of the EFT program files installation directory. Typically this will be **C:\Program Files\Globalscape\EFT Server\DBUtility**.

Requirements

- The utility requires the .NET Framework 4 (Full version)
- When operating against an Oracle database, the utility requires the 32-bit version of the Oracle Data Access Components (ODAC)

Capabilities

The database utility is capable of performing the following tasks:

- Check the version of the database to see if it is up to date. This may be used to see if an upgrade must be performed on a database before it is ready to be used by EFT.
- Generate an SQL script that may be used to create a new database schema (tables, views, etc.) manually within an existing database.
- Generate an SQL script that may be used to upgrade an existing database schema manually.
- Analyze an existing database prior to performing an upgrade. The analysis will verify prerequisites, display information about the database, and display the SQL that will be used to upgrade the database.
- Upgrade an existing database schema to the latest version.

Logging

The utility is capable of outputting various levels of information ranging from errors to debug/trace level information.

By default, the utility will output errors, warnings, and informational messages to the command window. If the "-verbose" command line parameter is specified, the utility

will also output more fined-grained debug/trace level messages to the command window.

The utility may also optionally output to a log file as specified using the "-logfile" command line option. The output to the log file will include all levels of messages from errors to debug/trace level information.

SQL Scripts

The utility requires the presence of various SQL Scripts located in database-specific subdirectories to perform its actions. These subdirectories contain scripts such as:

- create_* - scripts used for creating new, clean database schemas for use by the EFT application
- Purge* - scripts that may be used for purging data from the database
- *ODBC - scripts that may be used to create the necessary tables to use an ODBC data source for user authentication
- upgrade_* - upgrade scripts for upgrading various versions of the database

By default, the utility will look for the "SQL Server" and "Oracle" directories under its current working directory. During installation of the Database utility, these script directories will be created under the <InstallDir>\DBUtility directory, so the scripts will be available to the utility.

If the utility is unable to locate these subdirectories, it will also look for the EFT "AppData" path in advanced properties and then look for the subdirectories under that location.

Additionally, the user may specify an alternate parent directory using the "-scripts" command line parameter.

Usage

The database utility is a command line utility and may be executed by opening a Windows Command Prompt and navigating to the "DBUtility" subdirectory of the EFT installation folder (for example, **C:\Program Files\Globalscape\EFT Server\DBUtility**) and running the command "DBUtility.exe."

Each of the scripts has comments at the top describing their usage.

Help

The utility includes built-in help documentation. Additionally, the utility will provide feedback on incorrect or missing command line parameters.

The built-in help documentation for the utility may be accessed using the command:

```
DBUtility.exe -help
```

More detailed help for the various top-level actions may be accessed using the command:

```
DBUtility.exe -help -action <Action ID>
```

Where <Action ID> is one of:

- **CheckVersion**- checks the version of the database to see if it is up to date
- **CreateScript**- generates a SQL script that may be used to manually create a new database schema
- **UpgradePreview**- used prior to upgrading a database. This action will generate and display useful pre-upgrade information as well as the actual SQL that will be used to upgrade the database
- **UpgradeSchema**- upgrades the database, if needed
- **UpgradeScript**- generates a script that may be used to manually upgrade a database

Examples

Example executions for each of the actions supported by the utility may be viewed in the command line help for each action.

DBUtility Command Line Parameters

The following section describes each of the command line parameters for the utility. Depending on the action performed, only a subset of the parameters will be applicable or required.

For the command line parameters that accept a value, the value should be enclosed in double-quotes if the value contains spaces. For example,

```
-logfile="C:\My Logs\MyLogFile.txt"
```

Parameter Definitions

- -help
  - Description: Display help on the command line. Refer to the "Help" section above for additional information.
- -logfile=<file>
  - Description: When specified the utility will log output of the execution to the specified log file.
  - Default: None
  - Example:

    ```
    -logfile="C:\My Logs\MyLogFile.txt"
    ```
- -optionsfile=<file>
  - Description: When specified the utility will load command line parameters from the file. The file should specify parameters in a "parameter=value" pair with one pair specified per line. Parameters specified on the command line override parameters specified in the file.
  - Default: None
  - Example:

    ```
    -optionsfile="C:\My Scripts\MyOptionsFile.txt"
    ```
- -scriptfile=<file>
  - Description: For actions that generate output SQL scripts this parameter defines the file to which the script should be written.
  - Default: None
  - Example:

    ```
    -scriptfile="C:\My Scripts\MySQLScript.sql"
    ```
- -errorfile=<file>
  - Description: When specified the utility will log terminal errors to the specified file. Mainly used for error handling when the utility is called by the EFT installer.
  - Default: None
  - Example:

    ```
    -errorfile="C:\My Scripts\MyErrorFile.txt"
    ```

- - resultfile=<file>
    - Description: When specified the utility will output result status codes for the execution to the file. Mainly used for state handling when the utility is called by the EFT installer.
    - Default: None
    - Example:

      ```
      =resultfile="C:\My Scripts\MyResultFile.txt"
      ```
- -pause
    - Description: When specified the utility will pause at the end of the execution. Useful when executing the utility through a shortcut to keep the console window from closing before the user has a chance to review the results.
    - Default: None
- -verbose
    - Description: When specified the utility will output additional debug level logging.
    - Default: None
- -action=<id>
    - Description: Specifies the overall action to be performed by the utility.
    - Valid values:
        - **CheckVersion**- checks the version of the database to see if it is up to date
        - **CreateScript**- generates a SQL script that may be used to manually create a new database schema
        - **UpgradePreview**- used prior to upgrading a database. This action will generate and display useful pre-upgrade information as well as the actual SQL that will be used to upgrade the database
        - **UpgradeSchema**- upgrades the database, if needed
        - **UpgradeScript**- generates a script that may be used to manually upgrade a database
    - Default: None
    - Example:

      ```
      -action=UpgradeSchema
      ```

- -type=<type>
  - Description: The dialect of the database.
  - Valid values:
    - SQLServer - a SQL Server/SQL Server Express database
    - Oracle - an Oracle database
  - Default: None
  - Example:

    ```
    -type=SQLServer
    ```

- -server=<server>
  - Description: The database server host or IP address
  - Default: None
  - Example:

    ```
    -server="Jupiter"
    ```

- -port=<port>
  - Description: The listener port for the database on the database server/host.
  - Default: None
  - Example:

    ```
    -port=1433
    ```

- -instance=<instance>
  - Description: The database server instance name.
  - Default: None
  - Example:

    ```
    -instance="MSSQLSERVER"
    ```

- -database=<database>
  - Description: The name of the database.
  - Default: None
  - Example:

    ```
    -database="GLOBALSCAPE"
    ```

- -timeout=<timeout>

  - Description: The timeout, in seconds, to continue trying to connect to the database. A value of 0 causes the utility to wait indefinitely and should be used with caution.
  - Default: 30 seconds
  - Example:

    ```
    -timeout=5
    ```

- -auth=<auth>
  - Description: The type of authentication to use when connecting to a SQL Server database.
  - Valid values:
    - SQLServer - Use SQL Server authentication which requires specification of the username and password.
    - Windows - Use Windows authentication which will use the currently logged in user account.
  - Default: None
  - Example:

    ```
    -auth=SQLServer
    ```

- -user=<user>
  - Description: The login name to use when connecting to the database.
  - Default: None
  - Example:

    ```
    -user="eftdbuser"
    ```

- -pass=<pass>
  - Description: The password to use when connecting to the database.
  - Default: None
  - Example:

    ```
    -pass="3qym9NCebHDJ"
    ```

- -scripts=<dir>
  - Description: Parent directory containing the SQL Server and Oracle SQL Scripts subdirectories. Refer to the "SQL Scripts" section above for additional information.
  - Default: Refer to the "SQL Scripts" section above for additional information.
  - Example:

    ```
    -scripts="C:\ProgramData\Globalscape\EFT Server"
    ```

Advanced Parameter Definitions

The following parameters are typically reserved for use by the EFT installer and will normally not be useful to end users. However, they are documented here for completeness.

- -conn=<connection string>
  - Description: When specified this string will be used as the full connection string to the database rather than constructing the string based on the distinct parts.
  - Default: None
  - Example:

    ```
    -conn="Data Source=(DESCRIPTION=(ADDRESS_LIST=
    (ADDRESS=(PROTOCOL=TCP)(HOST=mth-oracle)(PORT=1521)))
    (CONNECT_DATA=(SERVICE_
    NAME=orastart)));PersistSecurity
    Info=true;User Id=eftdbuser;Password=3qym9NCebHDJ"
    ```

- -app=<application name>
  - Description: The application name to present to the database for use when identifying connections.
  - Default: None
  - Example:

    ```
    -app="EFT Database Utility"
    ```

- -installerdir=<directory>
  - Description: The directory containing the EFT Installer. May be used during some upgrades for accessing or storing additional files.
  - Default: None
  - Example:

```
-installerdir="C:\Users\administrator\AppData\Local\Temp\
nsdB57C.tmp"
```

- -installationdir=<directory>
  - Description: The directory where EFT is installed or will be installed. May be used during some upgrades for accessing or storing additional files.
  - Default: None
  - Example:

    ```
    -installationdir="C:\Program Files\Globalscape\EFT
    Server"
    ```

- -appdatadir=<dir>
  - Description: The directory that will be used for the EFT application data. May be used during some upgrades for accessing or storing additional files.
  - Default: None
  - Example:

    ```
    -appdatadir="C:\ProgramData\Globalscape\EFT Server"
    ```

- -backupdir=<dir>
  - Description: The directory in which to store backup data. May be used during some upgrades.
  - Default: None
  - Example:

    ```
    -backupdir="C:\ProgramData\Globalscape\EFT
    Server\Backup"
    ```

EFT DB Files

When you configure the server's administration access, all of this data from the server, the site, DMZ Gateway, protocols, users, and so on, is written into ".DB" files and is stored in the **\ProgramData**folder (by default, **C:\ProgramData\Globalscape\EFT Server**). Having all of the settings in these files will help with migrating Sites between different EFT instances. (That is, copying the files to another computer, and making some adjustment if necessary (like paths), and importing it to new instance.)

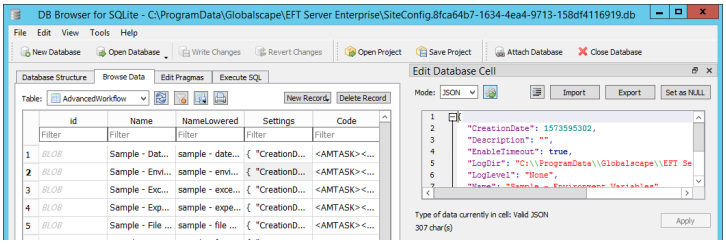
> **NOTE:** DB Browser for SQLite displays text in UTF-8 encoding (which includes ASCII as subset). But your data could be stored in other encodings, like ISO-8859-1 or IBM851. In that case, the encoding has to be indicated to the data browser, otherwise the cell contents could be displayed as "BLOB".

- The .DB files are not in a human-readable format in text editors or other such tools. Instead, you can use a tool like DB Browser for SQLite to view or export the .DB files. You can export a .DB file as a JSON or other formats.
- The date stamps in the .DB files are "epoch" dates. If needed, you can convert epoch to human-readable date (and the reverse) using a conversion tool such as https://www.epochconverter.com/.
- The DB Browser for SQLite is a spreadsheet-like interface that provides access to the full capability of the underlying SQLite database. Some of the EFTDB-specific features are described below. For more information about using DB Browser, refer to the DB Browser documentation.
- Download and install the latest Windows release of DB Browser on the EFT computer.
- **ServerStats.db** and **SiteStats.db** contain statistics about the Server and Site from which you can generate data to provide to Globalscape Support when troubleshooting Server or Site problems. When EFT is running, it writes to these tables once an hour, one ROW for each occurrence. The snapshot interval can be changed with an advanced property, **StatisticsAuditInterval**, which is 60 minutes by default. The shortest interval allowed is 1 minute. If it is set to 0, then EFT will use the default of 60 minutes.
- The **Timestamp** column is an "epoch" date/time, as described above.
- **ServerConfig.db** contains configuration information found on the Server tabs, such as server status, listening IP, administrator access and permissions, SSL, FIPS, logs, database settings, SMTP settings, and HA information.
- **SiteConfig<GUID>.db**contains configuration information found on the Site tabs, such as Site connection information, security settings, web portals configuration, and Content Integrity Control configuration.

- The **SSLCert**table does not contain SSL certificates. Those are still saved as .crt/.key files in the EFT **\ProgramData**directory, or wherever you choose to save them.
- The **AdvancedWorkflow**table contains the built-in Sample Workflows and any that you create. You can import and export the Workflows as JSON files from within DB Browser for SQLite.

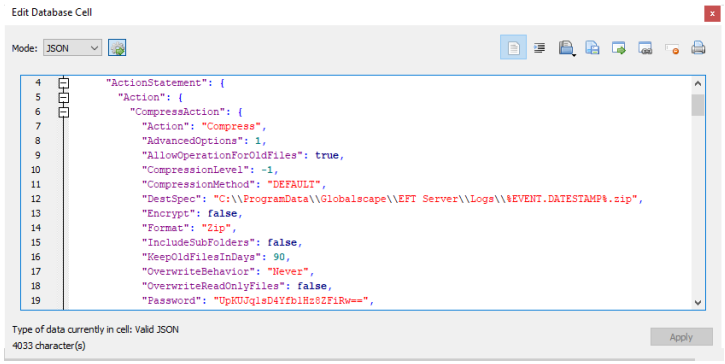
To use DB Browser for SQLite

1. In Windows Explorer, navigate to the EFT **\ProgramData**folder (for example, **C:\ProgramData\Globalscape\EFT Server**), right-click an EFT DB file, then click **Open with**.
2. Click **More apps** and select the **Always use this app to open .db files** check box.
3. Click the DB Browser short-cut icon. DB Browser opens to the **Database Structure** tab.
4. On the main menu, click **View** to choose which panels on the right to show or hide. (Click **Window Layout > Reset Window Layout** to go back to the default.)
    - The **Database Structure** tab shows each of the database tables. If you make dialog box larger or scroll to the right, you can see the **Schema** column.
    - To browse the data in the database, click **Browse Data** then click in a cell. The data of the cell appears in the **Edit Database Cell** pane.
    - Click the **Open Database**icon, or **File > Open Database**, or **CTRL+O**. If you want to open read-only, click **File > Open Database Read Only**.



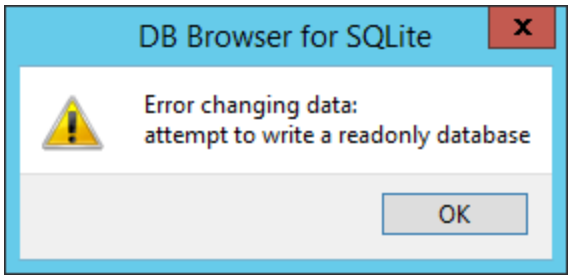
To view the data

1. Click the **Browse Data** tab, then click a data cell to view the content. For example, in the Site config db file, click the Table drop-down list, then click **EventRule**.
2. In the **EventRule** table, click the row for **Backup and Cleanup**, then click the **Trigger** column.
3. In the right pane, view the **Edit Database Cell** dialog, and you can view the structure of the event rule.

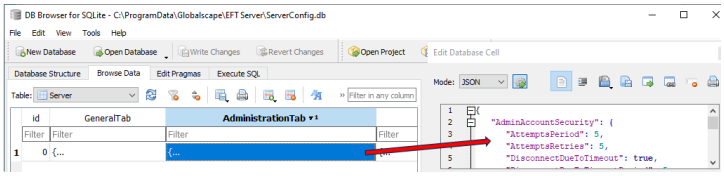


4. If you don't see the **Edit Database Cell** dialog box, press CTRL+E.
5. To reset the panels to their default locations, click **View > Window Layout > Reset Window Layout** , or press ALT+0.

   Unless you are viewing read-only or if the EFT server service is stopped, you can make edits in this window. Otherwise, an error message appears.



6. Many tables will display a left curly brace and an ellipsis {... to indicate there is more information. Click the cell, and the contents will be displayed in the **Edit Database Cell** pane/dialog box, as shown below.



*In the image above, the **AdministrationTab** cell is selected. The contents of the cell are displayed in the **Edit Database Cell** pane .*

Related Topics

- Viewing Data in DB Browser
- Generate Support Data

Database User Account Privileges

The database user account used by EFT must have certain privileges within the database for the application to function correctly. Additionally, a different set of privileges are needed for Installation, Upgrade, and Runtime, as described below.

Installation—When creating a new database, the EFT installer is capable of creating the database user account for you. Alternatively, you may create the database user account ahead of time. Either way, the EFT database user account must have certain privileges during the creation process. Once the creation process is complete, the privileges may be reduced to those necessary for runtime operation. (Refer to Runtime below.)

The following privileges, or their equivalents, are required during the creation process:

- SQL Server—The database user account must have the "db_owner" database role membership.
- Oracle—The database user account must have the following privileges:
  - CREATE SESSION
  - CREATE TABLE
  - CREATE TRIGGER
  - CREATE SEQUENCE
  - CREATE PROCEDURE
  - CREATE VIEW

Upgrade—When upgrading the ARM database, either through the EFT Installer or the Database Utility found in **C:\Program Files\Globalscape\EFT Server\DBUtility**, you should use the EFT database user account to connect to the database to perform the upgrade. The upgrade process may temporarily require that additional privileges be temporarily given to the EFT database user account. The actual set of privileges depends on the version of the database schema being upgraded. Before upgrading the database, the EFT Installer will perform an analysis of the database. Additionally, the "UpgradePreview" action may be used with the Database Utility to perform the analysis.

Part of this analysis will verify that the database user account possesses the necessary privileges to perform the upgrade. The analysis results will display any privileges that the account is lacking. **You will need to grant the appropriate privileges to the account temporarily before proceeding with the upgrade.** These privileges may be revoked once the upgrade process is complete. Refer to the Runtime section below for the privileges required during subsequent operation of EFT. To minimize the chance

of encountering missing privileges, you should grant the privileges described in Installation, above, before performing the upgrade preview analysis.

Runtime—During normal operations, the EFT only manipulates the data within the database while auditing, and so requires less powerful privileges. EFT does not modify the database schema during normal operation. If you want to lock down the EFT database user accounts during normal operation, ensure that the following minimal privileges, or their equivalents, are granted to the account:

- SQL Server—When operating against SQL Server, the EFT database user account only needs to be able to read data, write data, and execute stored procedures. The following permissions are required during normal operation:
    - CONNECT
    - DELETE
    - EXECUTE
    - INSERT
    - SELECT
    - UPDATE
- Oracle—During normal operation, the EFT database operates only within its own schema. Additionally, it has no need to create objects during runtime. Only the following privilege is required during normal operations:
    - CREATE SESSION

ARM Database Maintenance

The EFT administrators can enable database maintenance from the **Server > Logs** tab, in addition to the REST API (in Site configuration). The feature is disabled by default.

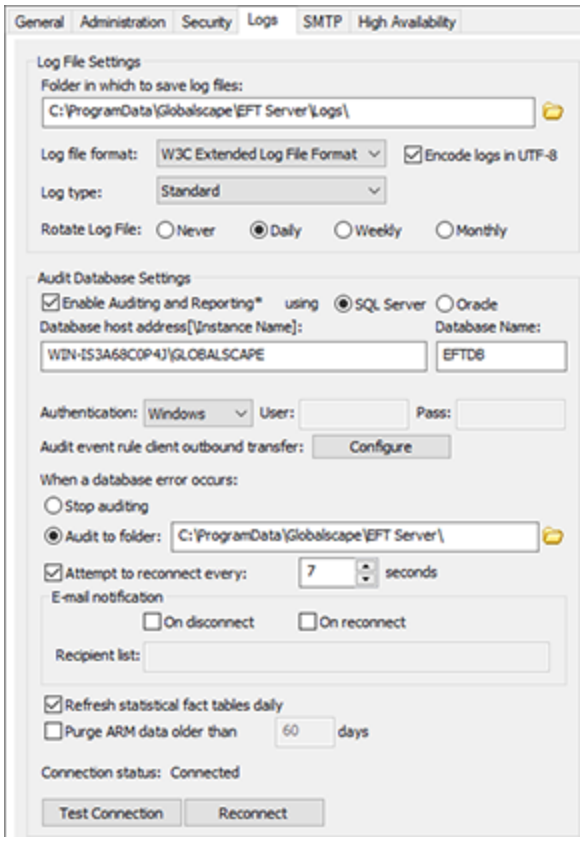
> **NOTE:** Available for SQL Server databases only. The Auditing and Reporting module must be licensed.

Space requirements for transactions in the ARM Database depend on the estimated EFT activity, number of users, and installed modules. A general estimate is 3MB to 5MB of per 1000 files uploaded. A minimum of 3GB hard drive space is recommended for the initial database size, with additional space required for growth over time. As your database continues to grow, it is necessary to purge old records periodically.

The helper script in **\ProgramData\Globalscape\EFT Server\SQL Server\Helper scripts\PurgeEFT.sql** describes in which order to run the scripts to improve database performance.

To enable and configure database maintenance

1. Administrator is presented with a call to action to opt-in to the purges.
2. On the **Server > Logs** tab, in the **Audit Database Settings** section, specify the number of days of retention.



Any data older than the number of days of retention must be purged. The default is 60 days, due to the complexities around running large reports in EFT.

To minimize impact to performance while the server is running, it will only delete 10 days of data on each night. The amount of time it takes to purge depends on the number of days you have in the database. You have to consider how many days of data you have to start with and what you want to end up with. The number you end up with is the number of days the administrator enters into that field. The higher the number of days of data you start with, the longer it will take to purge (especially if you've never purged). AFTER the first purge, and if you leave this enabled, EFT will continue to purge up to 10 days every night and therefore will never keep more days than the number of days you have defined.

You can find a copy of the schema upgrade SQL script that creates this stored procedure in the EFT directory under SQL. (\ProgramData\Globalscape\EFT Server\SQL Server) which of course, you do not need to run manually if you enable the **Purge ARM data older than** check box.)

- Maximum value: There is no maximum value, as some customers have large retention policies.
- Minimum value: A minimum entry of 45 days is required.

3. EFT must continue to log to the ARM database during the purge.

4. EFT must perform the maintenance actions at midnight (server time) interval. This value is NOT configurable.
    a. EFT will purge ALL entries that are older than the number of days of retention specified when midnight (server time) starts.
    b. If the purge fails to purge all entries before the next run, an entry should be logged.

Upgrading the EFT Database

This introduction describes in general how an EFT database upgrade works.

You have the option of either upgrading the database during the upgrade process within the EFT Installer or choose to upgrade the database "out of band" later using the Database Utility. Because the EFT installer uses the same Database Utility internally to perform the upgrade, the methods are synonymous.

The ARM database schema maintains an independent version number. This version is used to determine if the database schema and data require an upgrade across various releases of the EFT application. This version number is maintained in a new table called "TBL_SCHEMA_VERSION." This new table is created as part of the initial ARM upgrade process when upgrading EFT.

> **NOTE:** When you upgrade from 7.4.x to EFT v8.x, EFT configuration is moved from previous files to the DB files. All settings for the server, for each Site (Site settings, users, VFS, permissions, etc.), and for Workspaces are in .DB files.

During the upgrade, you will be prompted to provide the user credentials that should be used when connecting to the database. **You must provide the credentials for the EFT database user account, as opposed to the super-user accounts such as "sa" or "sys"**, because the upgrade process assumes it is operating as the database account that owns the schema to be upgraded. (Refer to Database User Account Privileges > Upgrade for information on the required database user account privileges necessary to successfully upgrade.)

When upgrading from within the EFT installation process, the installer will analyze the database prior to performing the actual upgrade. The results of this analysis are displayed in an upgrade preview page of the installer. Administrators are urged to read the results carefully prior to continuing with the upgrade. (EFT's upgrader does not check the database for fragmentation.)

The analysis step will determine whether the database requires an upgrade by examining the version number in the new version table. Across many builds and releases of the EFT application, the ARM database may not require any changes. As such, the version number for the database may not change as often as the EFT version. If the database does not require an upgrade, then the installer will state this and essentially skip the ARM upgrade process.

As with the database upgrade, the database analysis process used in the EFT installer is actually performed by the Database Utility and is equivalent to running the utility with the "-action=PreviewUpgrade" command line option. In addition to checking the database version number, the installer will also check for various prerequisites needed

to perform the upgrade. Prerequisites that have been met will be displayed with a "PASS" status. Any prerequisites that have not been met will be displayed with a "FAIL" or "WARN" status. These issues should be researched and rectified prior to proceeding with the upgrade.

Recommendations are provided along with any failed prerequisites suggesting how to resolve the issue. After remedying any errors, you can run the analysis again by clicking **Reanalyze**.

The analysis will also display information about the database such as the approximate size of the user data as well as the age of the user data within the database. Additionally, the SQL script that will subsequently be used to perform the actual upgrade will be displayed.

You may decide to upgrade the database later. If so, you can retain the upgrade script by clicking **View** to open the database analysis results in a text editor and then save to a file of your choosing.

Alternatively, you can run the EFT installer in maintenance mode or run the Database Utility using the "-action=UpgradeSchema" option to upgrade the database another time.

User Account Permission or Privilege Requirements

When upgrading the ARM Database, you should use the EFT Database user account to connect to the database to perform the upgrade. This is as opposed to using one of the more privileged system accounts such as the "sa" account on SQL Server or the "sys" or "system" accounts on Oracle.

For additional information related to database user account privileges refer to Database User Account Privileges.

SQL Server

The user account used to upgrade the database should have the "db_owner" privilege. This is the default for the user account created for, and used by, the EFT. As such, no action is required on your part prior to upgrading.

Oracle

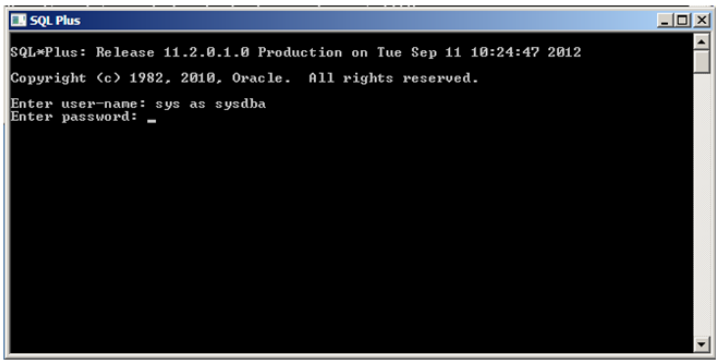
The ARM module makes use of database views. In previous releases, the database user account created for use by the EFT was not granted the ability to create views. As such, prior to upgrading an Oracle ARM database, you must grant this privilege to the EFT database user account manually. This is done by granting the "CREATE VIEW" privilege to the account using a more privileged account such as the "sys" or "system" account.

One method of granting the privilege is to connect to the database using the Oracle command line "SQL Plus" utility. On the computer where Oracle is installed, launch the SQL Plus utility:

- Click the SQL Plus **Start** menu shortcut (for example, **Start Menu > All Programs > Oracle - OraDb11g_home1 > Application Development > SQL Plus**)
- If the utility is available on the system path, then open a Windows command prompt (for example, **Start > Run > cmd.exe**), type `sqlplus` at the command prompt, and then press ENTER.

Once SQL Plus has started, you will be prompted for login credentials. Connect using a privileged account such as "sys" or "system". Be aware that when connecting as the "sys" account you must provide the "as sysdba" option; for example:

```
sys as sysdba
```



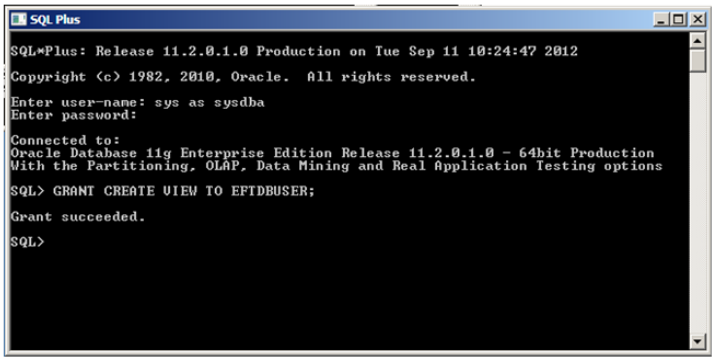
Complete the login process by providing the password.

Use the following command to grant the "CREATE VIEW" privilege to the EFT database user account:

```
GRANT CREATE VIEW TO <User>;
```

Where <User> is the name of the EFT database user account. For example:

```
GRANT CREATE VIEW TO EFTDBUSER;
```



Exit the SQL Plus tool by typing `Exit` and pressing ENTER.

Time Requirements

The time it takes to perform the upgrade depends both on the size of the database and the performance characteristics of the computer on which the database resides.

Our internal testing has shown that the database upgrade can take as little as 15 minutes for a moderately sized database of 5GB, up to 3 hours or longer for larger databases of 30GB or more. Because the time it takes to perform the upgrade is greatly dependent on CPU and Disk I/O speed, it is difficult to provide an exact time for any given situation.

For additional information related to upgrading large databases please refer to Upgrading Large Databases.

Refer to Upgrade Paths below for a discussion of the available upgrade paths that may be used to minimize down time.

Disk Space Requirements

The size of the database will grow as part of the upgrade because of changes in the data types used for storing character-based data.

Our internal testing indicates that, on average, the size of user data in the database will increase by approximately 31% as part of the upgrade process. For example, if your database consumes 10GB before upgrading, then it will use approximately 13GB after upgrading.

If disk space is limited, you should consider purging older data from the database prior to upgrading. For information on purging data from the ARM database, refer to ARM Database Maintenance.

For additional information related to upgrading large databases, refer to Upgrading Large Databases.

SQL Server Considerations

If you have limited disk space and are using SQL Server, it may be possible to reduce the size of the database prior to proceeding with the upgrade. This may be accomplished by "shrinking" the database, which will reclaim unused space.

For information and considerations on shrinking a SQL Server database, please refer to the Shrink a Database topic on the Microsoft Developer Network site.

During the upgrade process, the increase in size of the user data will be reflected by an increase in the size of the database's MDF file by approximately 31%.

Additionally, the database transaction log file, the LDF file, may temporarily grow in size. In testing, the LDF file typically increased to between 1% and 3% of the starting size of the corresponding MDF file. For example, if your MDF file is 10GB in size, then the LDF file could be expected to grow temporarily to approximately 300 MB in size.

Oracle Considerations

When upgrading Oracle databases you must ensure that not only is the appropriate amount of disk space available, but that the USERS tablespace is capable of growing to accommodate the additional storage requirements. You may consider allowing the USERS tablespace data files to auto extend during the upgrade process. Additionally it may be necessary or desirable to create additional data files for use with the USERS tablespace.

Upgrade Paths

Depending on the size of the ARM database and the time constraints on performing the upgrade of EFT, you may choose to consider alternate methods of upgrading the ARM database. Described below are pros and cons of two alternate methods of upgrading the database, when each method is appropriate, and how to perform the upgrade using each method.

Method 1: During the EFT upgrade

This is the typical method of upgrading the ARM database. When running the EFT installer, you can upgrade the ARM database as part of the full upgrade process.

Pros

- Simplest method, requiring minimal manual steps

Cons

- The EFT will be unavailable for the time it takes to perform the entire upgrade

Appropriate When

- The ARM database is relatively small or the computer running the database is sufficiently powerful
- The ARM database is large, but a few hours of downtime is acceptable

How to Perform

- When upgrading using the EFT installer, on the **EFT Auditing and Reporting database configuration** page of the wizard, click **Configure Auditing and Reporting** and proceed accordingly.

Method 2: Out of band

With this method, EFT may be upgraded independent of the ARM Database. Specifically, you would upgrade EFT using the EFT installer application, but choose to skip upgrading the ARM database at that time. Once the EFT application has been upgraded, it may be restarted and will thus be available to service end users. During the time that the ARM Database has not yet been upgraded, the EFT application can temporarily store audit information to disk.

You can then upgrade the ARM database using the Database Utility. Once the upgrade has completed, the EFT will then be able to reconnect to the database as normal.

Pros

- Allows for minimal downtime of the main EFT facilities

Cons

- EFT Reporting capabilities will be temporarily unavailable
- Requires additional steps to perform the upgrade

Appropriate When

- Upgrading very large database and the necessary downtime of the main EFT facilities is unacceptable

How to Perform

- Prior to starting the upgrade process, configure the EFT application to audit to a folder while disconnected from the database. Refer to Audit Database Settings for information about this functionality.
- Upgrade the EFT application using the EFT installer. On the **EFT Auditing and Reporting database configuration** page of the installer, click **Skip Auditing and Reporting configuration** and proceed accordingly.
- After EFT has been upgraded, restart the EFT service.
- Upgrade the ARM database using the Database Utility.
    - First, perform a preview upgrade using the "-action=UpgradePreview" option of the utility. This will verify that the appropriate requirements for upgrading the database have been met.
    - After the requirements have been verified, use the "-action=UpgradeSchema" option to perform the actual upgrade. Optionally you may instead generate an upgrade script using the "-action=UpgradeScript" option and manually upgrade the database

using vendor tools such as SQL Server Development Studio or SQL Plus.
- Refer to EFT Database Utility for additional information.

ARM Upgrade Checklist

SQL Server

- Ensure a current backup of the database is available
- If necessary or desired, purge older data from the database
- Ensure the necessary disk space is available to perform the upgrade
- Remove any custom schema modifications made to the database
- Follow the desired upgrade method
- Recreate any custom schema modifications

Oracle

- Ensure a current backup of the database is available
- If necessary/desired, purge older data from the database
- Ensure the necessary disk space is available to perform the upgrade
- Ensure the USERS tablespace and associated data files are configured to allow for the necessary data growth
- Remove any custom schema modifications made to the database
- Grant the "CREATE VIEW" privilege to the EFT database user account
- Follow the desired upgrade method
- Recreate any custom schema modifications

Related Topics

- Upgrading Large Databases
- Database User Account Privileges

Upgrading a Large Database

The majority of the modifications performed on the ARM database when upgraded take only minutes to complete. Occasionally, more modifications are needed when upgrading the database schema. These upgrades may take a long time, especially when they require modifications to the data stored within the database. As such, the time it takes to perform the upgrade may increase with the size of the database. Depending on the size of the database, such upgrades take hours instead of minutes.

The database upgrade preview process includes the age of the oldest data in the database as well as a rough estimate of the database size. Administrators should use this data to assess the current state of the database when deciding how and when to proceed with the database upgrade.

Administrators of large databases should consider the following options to ensure a smooth upgrade process:

- Administrators should consider purging older data from the database prior to upgrading. (Refer to***ARM Database Maintenance* on page 1832**for details.)
- The database should be backed up prior to any upgrade to allow for quick recovery in case of errors.
- Administrators should consider making a copy of the ARM database and performing a test upgrade of the database. The script necessary to perform the test upgrade may be obtained by proceeding through the EFT Installer's upgrade process and choosing to upgrade the ARM Database. When prompted for the database credentials, specify the test database credentials. On the **Upgrade Preview** page of the installer, click **View**, save a copy of the upgrade script, and then cancel the EFT installer. You may now use the SQL script to upgrade the database manually.

  Alternatively, you can install a clean copy of EFT on another computer and use the Database Utility found in **C:\Program Files\Globalscape\EFT Server\DBUtility**to perform the test upgrade.
- Administrators should consider upgrading the database out-of-band from upgrading the EFT installation. This may be done by skipping the ARM database upgrade in the EFT Installer when performing the initial EFT upgrade. The updated version of the EFT will temporarily audit database transactions to disk until the ARM database has been upgraded.

  To perform an out-of-band upgrade of ARM

  1. If desired, prior to upgrading the EFT, enable the ARM audit-to-folder feature.

2. Use the installer to upgrade the EFT, but skip the ARM upgrade process, then do one of the following:
    - Rerun the installer in maintenance mode later to upgrade the ARM database.
    - Use the Database Utility to perform the upgrade.
    - Manually upgrade using the SQL scripts generated by the Database Utility.
3. After the ARM database has been upgraded, click **Reconnect** in the EFT administration interface, on the Server's **Logs**tab to instruct EFT to connect to the upgraded database. EFT will then import any database transactions that were audited to disk in the interim.

Related Topics

- Upgrading the EFT Database
- EFT Database Utility
- Installing and Configuring the Auditing and Reporting Module
- ARM Database Maintanence

Manually Creating the ARM Database in SQL Server

Manually creating the ARM database in SQL Server is for advanced users who are well versed in SQL Server.

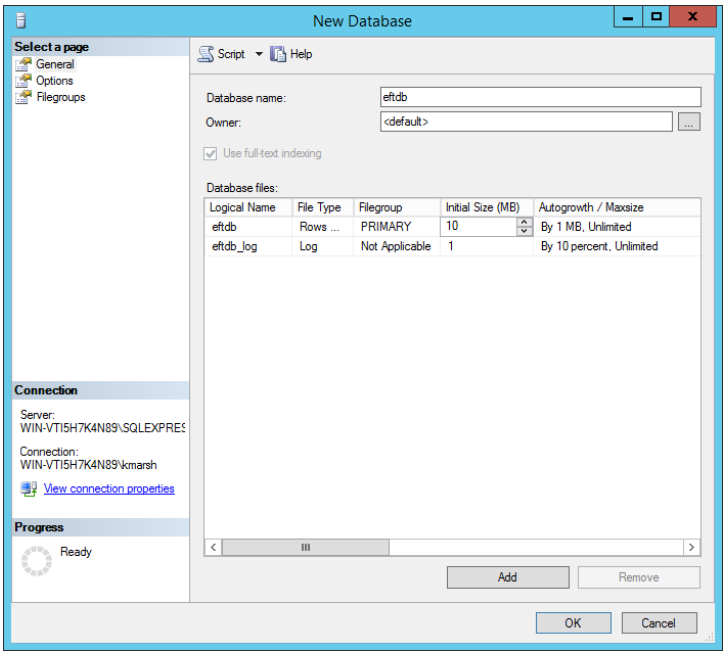
- **If you installed ARM when installing EFT**, the ARM database was created for you. During installation, all tables were created in the schema regardless of which features and/or modules are actually in use. You do not have to create them manually.
- **If you did not create the ARM database at installation**, you can use the installer at any time after the initial installation of EFT to create the database. Alternatively, this manual procedure can be used to create the database user account, create the schema, configure EFT to connect to the database, and then test the connection.

The following instructions use the SQL Server Management Studio application from Microsoft. Optionally, users may prefer to use command line tools such as oSQL to create the database. The oSQL utility allows you to execute Transact-SQL statements, system procedures, and scripts for creating and maintaining the database. For additional information on the oSQL utility, including common script samples, refer to osql Utilityon microsoft.com.

First you will create the database, then create the database user account, create the schema, configure EFT to connect to the database, and then test the connection.

To create the database

1. Using the SQL Server Management Studio application, connect to the SQL Server instance using an account that has the privileges necessary to create user accounts and databases. Typically the "sa" account will suffice.
2. In the left pane, right-click **Databases**, then click **New Database**.
3. The **New Database** dialog box appears. Name the database *eftdb.* (You can use a different database name, but be sure to use the name you chose throughout this procedure.)



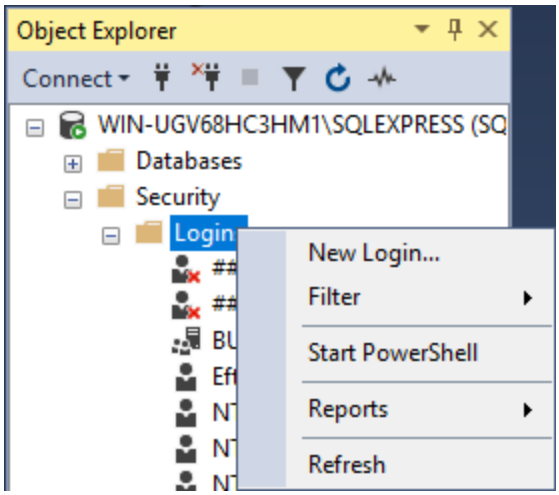
4. In the **Database files** table, change the **Initial size** value to 10 MB for the eftdb logical name (first row). Leave the **eftdb_log** row as is.
5. Click **OK** to finalize creation of the database.

Create the Database User Account

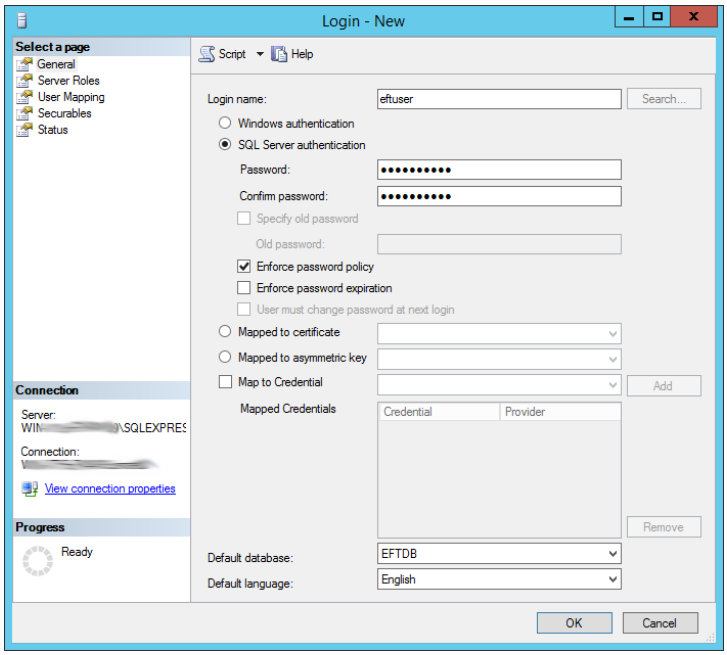
During installation, EFT needs full DB Owner access to the auditing database to set up the schema. During updates or upgrades, EFT needs full DB Owner access to update the schema. Once it is set up, EFT only needs to be able to read, write, and execute stored procedures. For more information on the required database privileges please refer to Database User Account Privileges.

To create the database user account

1. Using the SQL Server Management Studio application, connect to the SQL Server instance using an account that has the privilege to create user accounts and databases. Typically the "sa" account will suffice.
2. In the left pane, expand the **Security** node, right-click **Logins**, and then click **New Login**.



The **New Login** dialog box appears.

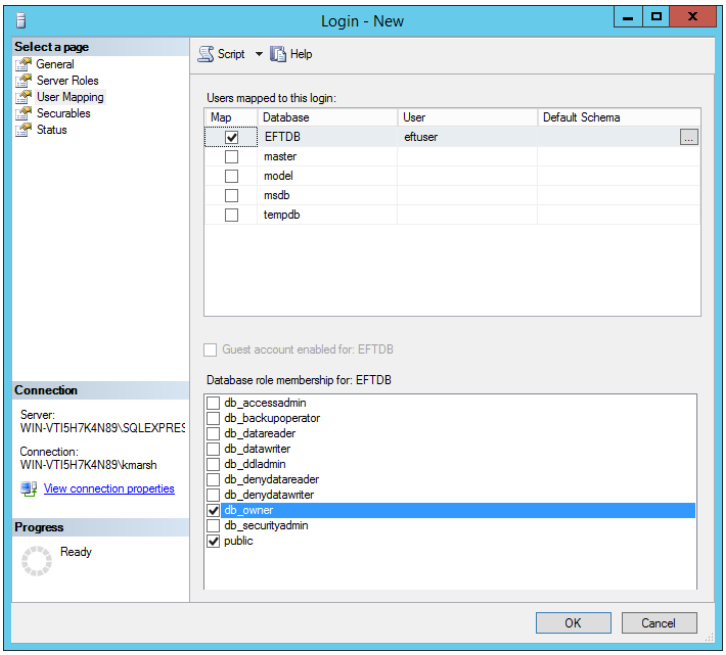


3. Create a new user called *eftuser*and then click **SQL Server Authentication**. (You can use a different user name, but be sure to use the same name throughout the procedure.)

   If SQL Server Authentication is not available as a choice, verify that the SQL Server has been configured to support mixed mode.

4. In the **Password**and **Confirm password** boxes, provide a complex password consisting of an alphanumeric and symbol mix of at least 8 characters.
5. Ensure the **Enforce Password Policy** check box is selected.

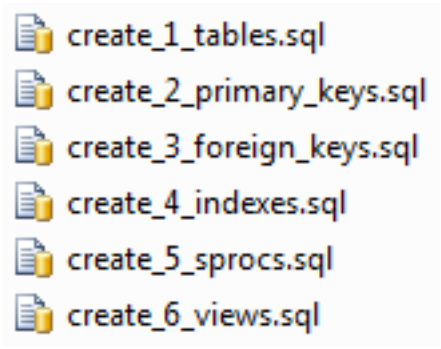
6. Ensure the **Enforce password expiration** check box is ***not***selected. (Optionally, you can enable this setting, but be aware that the *eftuser* account password will need to be changed periodically to prevent expiration.)
7. Ensure the **User must change password at next login** check box is ***not***selected.
8. Set the **Default**database to the **eftdb** database created earlier.
9. In **Default language**, click the list to select your language or leave it set to the <default> setting.
10. Select the **User Mapping**node in the left pane.
11. In the **Users mapped to this login** table, locate the entry for the eftdb database created earlier.
12. Select the check box in the **Map**column for the **eftdb** row and set the **Default Schema** to **dbo**.
13. While the **eftdb**row is selected, in the **Database role membership for** table, select the **dbo_owner**check box.



14. Click **OK** to finalize the user creation.

Create the Schema

During installation of the EFT, the installer will place a set of database creation SQL scripts in the **GlobalSCAPE\EFT Server\SQL Server** subfolder of the system **Program Data** folder. (Typically, **C:\ProgramData\GlobalSCAPE\EFT Server\SQL Server**.) The database creation scripts use the "create_#_" filename prefix. The # in the filename represents the order in which each script must be executed.



You will use these scripts to create the schema using the procedure below.

To create the schema

1. Using the SQL Server Management Studio application, connect to the SQL Server instance using an account that has the privilege to create user accounts and databases. Typically the "sa" account will suffice.
2. In the left pane, expand the **Databases** node, right-click on the **eftdb** node, and click **NewQuery**. A blank screen appears in the right pane in which you can type in a SQL query.
3. Execute each creation script in the specified order by copying/pasting the script file contents into the left pane and clicking **Execute**. A message appears each time you click **Execute**indicating whether the query was able to complete successfully.
4. In the left pane, expand **Databases**, then **eftdb**, then **Tables**. Verify that the database has populated correctly. (The tables defined in the script should have been created.)

Configure EFT

To configure EFT to connect to the newly created database, refer to Audit Database Settings.

To test the connection

1. Create a test connection with your FTP client to EFT and upload and download a few files.
2. In SQL Server Management Studio select the **dbo.tbl_ProtocolCommands**table under the **eftdb** database icon. It should return several rows with the commands issued by your client from the test connection.
3. You can now pull reports directly from EFT against data audited to SQL Server.

If you are running the administration interface, you must have an entry in that system's DNS for the name of the SQL Server, otherwise the administration interface will not be able to connect to the SQL Server when attempting to pull reports.

Manually Creating the ARM Database in Oracle

This procedure should only be used if you have not already created the ARM database using the EFT installer.

All tables will be created in the schema regardless of which features and/or modules are actually in use.

The following instructions assume you have already installed the Oracle database software and that an Oracle database is available. These instructions will make us of the Oracle SQLPlus command line utility to execute SQL against the Oracle database. Optionally, users may use an alternate utility of their preference.

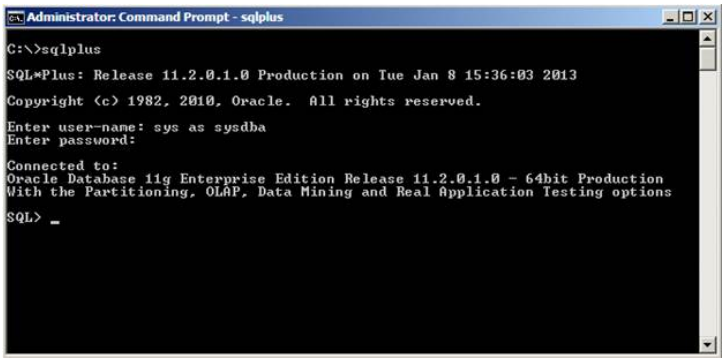
If you are running the administration interface, you must have an entry in that system's DNS for the name of the Oracle database computer, otherwise the administration interface will not be able to connect to the database when attempting to pull reports.

Create the Database User Account

During installation and upgrade, EFT needs creation privileges within the database. Once it is set up, EFT only needs to be able to read, write, and execute stored procedures. For the specific set of privileges required, please refer to Database User Account Privileges.

To create the database user account

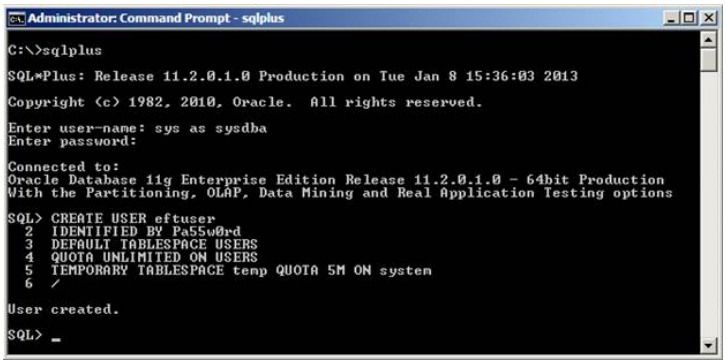
1. Using SQLPlus connect to the Oracle database using an account that has the privileges necessary to create user accounts and grant privileges. Typically the "sys" or "system" account will suffice. Note that when connecting as the "sys" account you will typically need to specify the "as sysdba" option.



2. Create the database user account by executing the following statement in SQLPlus, replacing `<username>` with the desired database user account name, such as `eftuser`, and `<password>` with the desired password.

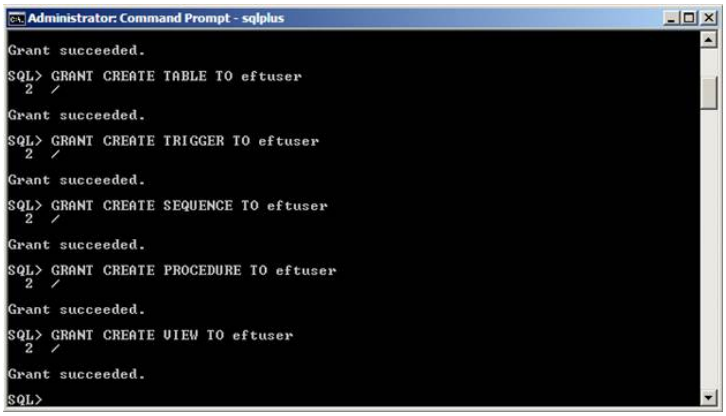
```
CREATE USER <username>
IDENTIFIED BY <password>
DEFAULT TABLESPACE USERS
QUOTA UNLIMITED ON USERS
TEMPORARY TABLESPACE temp QUOTA 5M ON system
/
```

For example:



3. Grant the necessary privileges to the database user account by executing the following statements in SQLPlus, replacing <username> with the username of the account you just created, such as eftuser.

   For example:

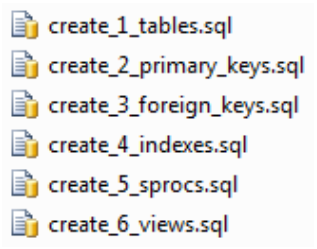


4. To exit SQLPlus, type `exit` and press ENTER.

Create the Database Objects

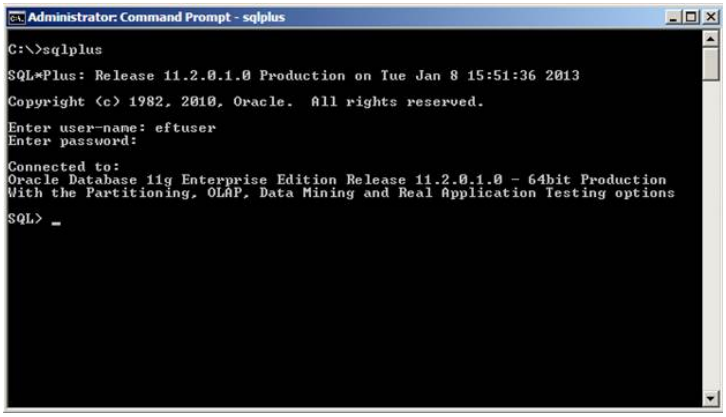
During installation of the EFT the installer will place a set of database creation SQL scripts in the **GlobalSCAPE\EFT Server\Oracle** subfolder of the system's **Program Data** folder. (Typically, **C:\ProgramData\GlobalSCAPE\EFT Server\Oracle**.)

The database creation scripts use the "create_#_" filename prefix. The # in the filename represents the order in which each script must be executed.



To create the database objects

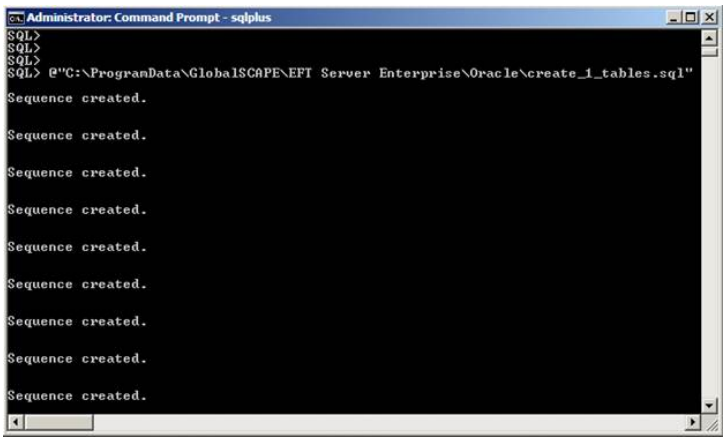
1. Using SQLPlus connect to the Oracle database using the EFT database user account created above.



2. In SQLPlus, execute each database creation SQL Script in the correct order using the command, replacing <Script File Path> with the full path and filename of the script.

```
@"<Script File Path>"
```

For example:



3. Once you have executed all of the creation scripts you may exit SQLPlus by typing `exit` and pressing ENTER.

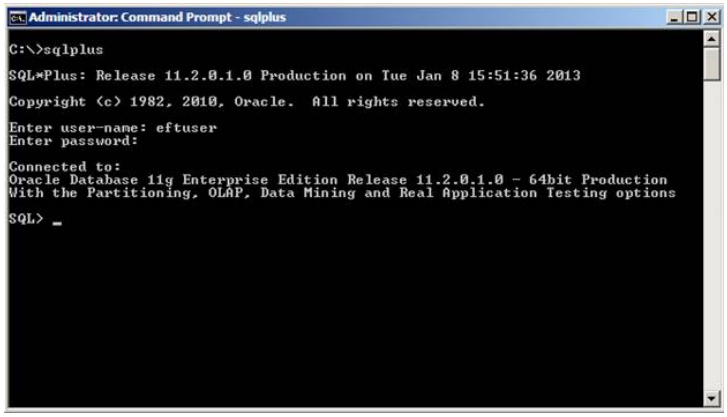
Configure EFT

To configure EFT to connect to the newly created database, refer to Audit Database Settings.

To test your connection

1. Create a test connection with your FTP client to EFT and upload and download a few files.
2. Using SQLPlus, connect to the Oracle database using the EFT database user account.

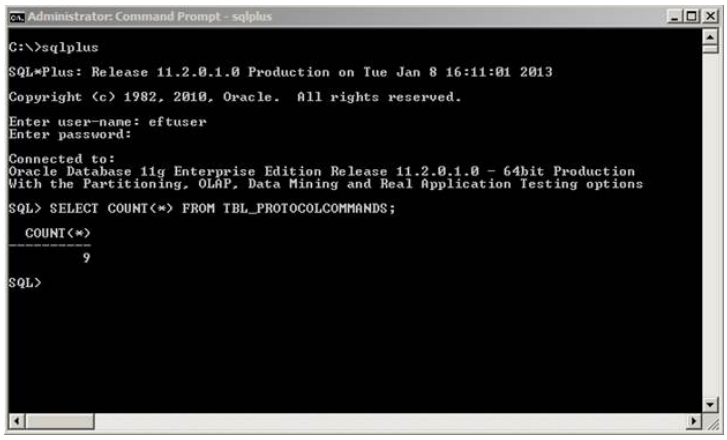
For example:



3. Retrieve the number of rows in the *TBL_PROTOCOLCOMMANDS* table by executing the following statement in SQLPlus:

   ```
   SELECT COUNT(*) FROM TBL_PROTOCOLCOMMANDS;
   ```

   For example:



   The above query should return a count of more than 0.

4. To exit SQLPlus, type `exit` and press ENTER.
5. You can now pull reports directly from EFT against data audited to Oracle.

Purging Data from the Database

Space requirements for transactions in the ARM Database depend on the estimated EFT activity, number of users, and installed modules. A general estimate is 3MB to 5MB of per 1000 files uploaded. A minimum of 3GB hard drive space is recommended for the initial database size, with additional space required for growth over time. As your database continues to grow, it is necessary to purge old records periodically.

The helper script in (by default) **C:\ProgramData\Globalscape\EFT Server\SQL Server\Helper scripts\PurgeEFT.sql** describes in which order to run the scripts to improve database performance.

Refer to ARM Database Maintenance to use the **Purge data older than n days** feature on the **Server > Logs** tab.

See also Knowledgebase article #10426: How can I purge EFT data from my ARM database?

Auditing

The topics below provide information about auditing EFT activity with the Auditing and Reporting module.

- Audit Database Settings
- Auditing Database Recovery
- FACT Tables
- Refreshing the FACT Tables
- How EFT Handles SQL Data
- Auditing Event Rule Actions
- Auditing Administrator Changes to the ARM Database
- ARM Database Maintenance
- Result IDs
- Auditing Database Errors and Logging
- ARM Database Schema Change Tracking

Related Topics

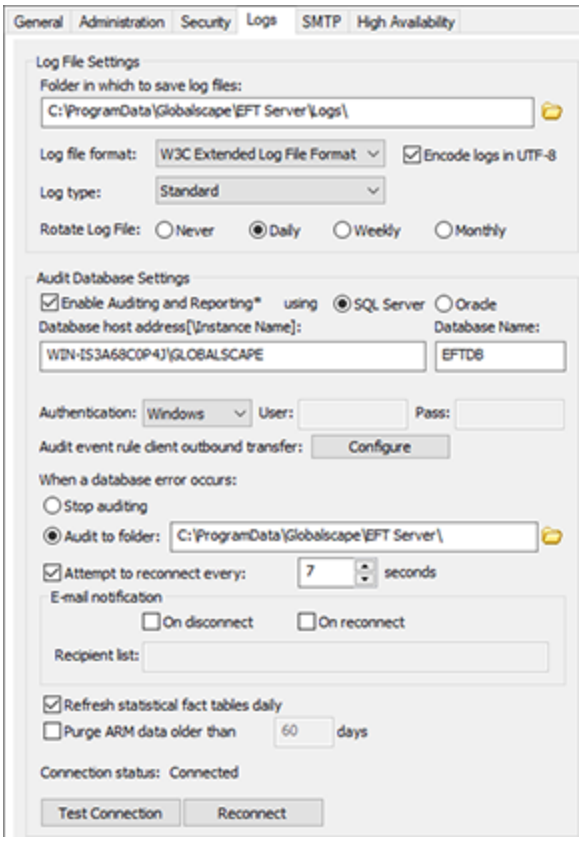
- Automating the Compliance Report
- PCI DSS Compliance Report

Audit Database Settings

When you run the Server Setup wizard, you are offered the opportunity to enable auditing and reporting and configure the connection information. If you chose to do that later or if you want to edit the database information, you can do so on the **Logs** tab in the **Audit Database Settings** area.

To enable and configure auditing and reporting

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node you want to configure.
3. In the right pane, click the Logs tab.



4. In the **Audit Database Settings** area, select the **Enable Auditing and Reporting** check box to enable communication with the database; clear the check box to disable auditing and reporting.
5. In the **Database type**area, select **SQL Server** or **Oracle**.

6. In the **Database host address[\Instance Name]** box, specify the host or database instance name of the database to which you want EFT to connect, or provide a DSN or DSN-less connection string. Refer to Establishing a System Data Source Name (DSN) or Using a DSN-Less Connection with ODBC Authentication, if you are using Audit Database Settings for your Site.
7. In the **Database Name**box, provide the name of the database or leave the box empty if you provided a connection string in the **Database host address [\Instance Name]** box.
8. For SQL Server databases, in the **Authentication**box, specify whether the database is to use **Windows Authentication** or **SQL Server Authentication**.
9. In the **Database username**and **Password** boxes, provide the username and password needed to connect to the database or leave the box empty if you provided a connection string in the **Database host address[\Instance Name]** box or if you are using Windows Authentication.
10. Next to **Audit event rule client outbound transfer**, click **Configure**, then specify whether to save Event Rule transfer failures to the database. Refer to **Event Rules (Automation) > Defining Event Rules >** Logging Event Rule Transfer Failures for details.
11. In the **When a database error occurs**area, specify whether you want to audit database errors to a folder:
    - If you do want to audit errors, or to stop it temporarily, click **Stop auditing**.
    - To **Audit to folder**, click the option, then specify the path to the folder in the box.
12. To automatically try to reconnect after an error occurs, select the **Attempt to reconnect every**check box and specify the frequency in seconds, from once every 7 seconds to once every 86,400 seconds (once per day).
13. In the **email notification**area, select the **On disconnect**check box and/or the **On reconnect**check box, and then in **Recipient list** specify one or more email addresses that you want EFT to send error notifications to in case of database failure. Multiple email addresses must be separated by semicolons **;** . When auditing is enabled, this email is sent any time that EFT cannot reach the database.
14. Select or clear the **Refresh statistical FACT tables daily** check box to indicate whether you want to refresh the FACT tables every night. Refer to Audit Database Settings for more information.
15. If you want EFT to automatically purge ARM data periodically, select the **Purge ARM data older than** check box, then specify a time period of 45 days or more. Refer to ARM Database Maintenance for more information.
16. If you make any changes to the database audit settings, click **Apply** to save the changes on EFT.

17. To verify the connection information, click **Test Connection**. The status of the database connection appears above the **Reconnect**button. If the database is not connected, click **Reconnect**to reconnect to the database.
    - **Test Connection** - EFT attempts a connection using the supplied parameters without applying the changes.
    - **Reconnect**- EFT applies the settings (a prompt appears if you made changes and did not click **Apply**) and attempts to connect to ARM with the new settings.

Auditing Database Recovery

If the auditing database has failed and EFT has been disconnected from the database for a while, you can prevent a loss of data by automatically saving auditing data to a text file when EFT is disconnected from the database. If EFT is configured to save auditing information to a text file, before reconnecting EFT to the database, repair the database, and then insert the data from the text file into the database. Then you can reconnect EFT to the database as described below.

The SQL statements logged in the text file must be loaded into the database before any reports are run.

If EFT is disconnected from the database and is configured to save auditing information to the log file, do the following:

1. Solve the connection problem.
2. Repair the database, and insert the data from the text file into the database. Be sure to insert the data only once, otherwise the auditing data will be corrupted.
3. In the administration interface, connect to EFT and click the **Server** tab.
4. On the **Server**tab, click the Server that you want to configure.
5. In the right pane, click the **Logs**tab and review the database connection information.
6. If you make any changes to the database host address, instance name, database name, etc., click **Apply** to apply these changes to EFT.)
7. Click **Test Connection** to test the status of the database connection.
8. The **Connection**status area indicates whether EFT is communicating with the database. To reconnect to the database, click **Reconnect**.

Fact Tables

Fact tables are really summary tables. From a SQL perspective, it is a group by of the regular ARM tables. This makes the tables smaller and faster to generate reports from. ARM groups the rows in the regular ARM table (detail table), so one row in the fact table represent many rows in an ARM table. Updating the fact tables could be seen as a pre-processing step to make the ARM reports faster. One example of this grouping is that ARM groups on date. While the detail tables have the time down to the second, the fact tables only show the date.

EFT database tables can grow very large. Fact tables are used to update EFT's tables every day and keep the database current. A check box on the**Server > Logs** tab, **Refresh facts table daily**, is selected by default.

- This feature is only available if the ARM database is managed in SQL Server. It is not available with Oracle databases.
- When the fact tables are enabled, a warning message explains that database performance can be affected temporarily while the tables are refreshed.
- The fact tables are updated as part of its hard-coded nightly cleanup routine (***not***the Cleanup Event Rule). There is no logging or reporting on the nightly fact tables cleanup.
- Upon new install, the initial fact table creation stored procedures are run, unless those tables already exist, and then will back-fill the fact tables with historical data
- The nightly import process logs in the ARM logger when it starts the job, with TRACE. If calling the DBUtility.exe fails, it will log an ERROR.

Each night, EFT imports data into its fact tables. Those tables are used to populate the following reports, all of which represent inbound behavior:

- Executive Summary Report
- Traffic - Average Transfer Rates by User
- Traffic - Connections Summary
- Traffic - Datewise-hourly Bytes Transferred
- Traffic - Datewise-IPwise Bytes Transferred
- Traffic - IPWise Connections (Summary)
- Traffic - Monthwise-IPwise Bytes Transferred
- Traffic - Most Active IPs - Connections
- Traffic - Most Active IPs - Data Transferred
- Traffic - Most Active Users - Connections

- Traffic - Most Active Users - Data Transferred (original report done)
- Traffic - Protocolwise Connections (Summary)
- Traffic - Sitewise-Hourly by User

Refreshing the FACT Tables

Rather than having to aggregate the data in real-time from the full set of data that may span multiple tables, "fact tables" are used to store daily pre-aggregated measurements, such as a daily record of “bytes transferred” for each user. These tables can alleviate load on the database server when running queries that are based off of these facts, as the reporting engine only needs to query sets of pre-aggregated data from an existing set of facts, resulting in lightning-fast reports.

By default, EFT will regularly update the fact tables so that EFT's analytics front end is always current.

The **Refresh fact tables** feature is only available if the ARM database is managed via SQL server; it is not available with an Oracle ARM database.

When the **Refresh statistical fact tables daily** check box is selected, EFT will refresh the fact table. Clear the check box if you do not want to refresh the fact tables.

- EFT will run the initial fact table creation stored procedures during installation, unless those tables already exist, in which case EFT will back-fill the fact tables with historical data.
- Fact table refreshes can severely affect database performance for a few minutes to several hours, depending on the volume of data audited since the last refresh.
- EFT will update the fact tables as part of its hard-coded nightly cleanup routine (at midnight).
- Using a SQLite databases viewer, in the ServerConfig.db, you can verify the ARM configuration data. In this you will find the **RefreshFactTables** value (true or false).
- When creating and configuring an EFT server administrative connection, the **Refresh statistical fact tables daily**check box is selected by default.

How EFT Handles SQL Data

EFT truncates data values within each audited SQL transaction to ensure the data value fits within the corresponding database field.

The special characters (as defined by the SQL interpreter) within each data value of an audit SQL event are escaped to ensure the data value is stored and retrieved properly from the database. The following special characters are escaped by EFT during generation of SQL statements prior to submission to the database engine:

- Single quote - %
- Open brace - [
- Percent - %
- Underscore - _

Auditing Event Rule Actions

Actions are audited to the Auditing and Reporting Module (ARM) database. For all Event Actions, the following items are audited:

- Time stamp
- Site Name
- Event Name
- Action Types such as move, copy, OpenPGP, and send email.
- Action Parameters - These are runtime values passed to the Action, not the replacement variables. For Advanced Workflow Actions, this is the path to the temporary file associated with the Workflow that was executed. This file contains more detailed debug logging if enabled for that particular workflow.
- Failed Action Flag - This is captured if this Action is the result of a FAILURE sequence on a prior Action.
- Action Result Code
- Result

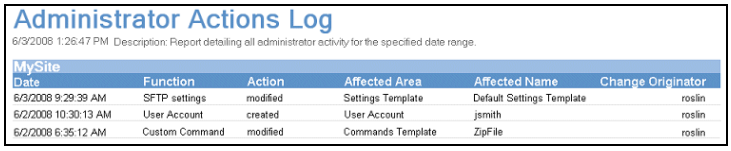
Auditing Administrator Changes to the ARM Database

(Requires ARM) Administrators often need to know when and what changes were made to EFT and who made them. The *administrator Actions Log* report provides information about administrator changes. When ARM expires, administrator changes are no longer audited.

EFT logs to the ARM database the following changes made to EFT:

- The **Date** the action occurred, in MM/DD/YYYY HH:MM:SS format.
- The affected feature or **Function**. (Refer to Functions Audited below.)
- The type of **Action**(created, added, removed, modified, enabled, disabled, started, and stopped).
- The **Affected Area**(Server, Site, Settings Template, User Account, Event Rule, Command, Group, VFS, Report).
- The name of the affected object, **Affected Name** (Server Name, Site Name, Settings Template Name, User or administrator Account Name, Event Rule Name, Command Name, Group Name, Folder Name, Report Name).
- The name of the administrator that made the change, **Change Originator**.

The data in the preconfigured report is arranged in columns, **Date**, **Function**, **Action**, **Affected Area**, **Affected Name**, and **Change Originator**, grouped by Site name, and sorted in reverse chronological order (newest change at the top).



Administrator Actions Log

6/3/2008 1:26:47 PM Description: Report detailing all administrator activity for the specified date range.

MySite

Date	Function	Action	Affected Area	Affected Name	Change Originator
6/3/2008 9:29:39 AM	SFTP settings	modified	Settings Template	Default Settings Template	roslin
6/2/2008 10:30:13 AM	User Account	created	User Account	jsmith	roslin
6/2/2008 6:35:12 AM	Custom Command	modified	Commands Template	ZipFile	roslin

Functions Audited

When the following functions are created, added, removed, modified, enabled, disabled, started, or stopped, the action is logged to the database. Many possible actions are grouped together. For example, modifying SSL cipher selection, changing SSL clear command channel values, or modifying SSL connection string all fall under "SSL settings." Also, intermediate states are not audited (for example, a toggle was checked, but later unchecked, rendering the transaction moot). Instead, only committed states are captured (once the administrator applies changes).

• SFTP protocol • SFTP settings • SFTP key • SFTP authentication settings • SSL protocol	• Password • Password complexity • Password reset • Password expiration • Password History	• SMTP settings • DoS prevention settings • Delegated administrators • Server • Site
• SSL settings • SSL require client certificate • SSL certificate • SSL authentication settings • FIPS mode for SSL	• Password initial reset • Invalid login settings • Inactive account settings • Account expiration settings • Connection limits	• Settings Template • User Account • Real-time monitoring • User kicked • Web Services Interface
• FIPS mode for SSH • HTTPS protocol • HTTPS settings • HTTP protocol • FTP Implicit Protocol	• Transfer limits • Disk limits • File type limits • IP address ban list • Group assignment	• Site root folder • Site listening IP • Custom command • Event Rule • Physical folder

• FTP Explicit Protocol • FTP protocol • FTP settings • AS2 protocol • AS2 settings	• Group (Permission) • Data sanitization (wiping) • DMZ Gateway • DMZ Gateway settings • Authentication settings	• Virtual folder • Folder permissions • administrator • Database refresh • Server service settings
• PASV port mode settings • Streaming repository encryption (EFS) • OpenPGP settings • OpenPGP key • Web Transfer Client	• Remote administration • Auditing settings • Log settings • Default Configuration File Path • Default User Database Refresh Interval	• Show Time In UTC/GMT • Ban On Invalid Login Settings • Advanced Workflows Task • Account details

Result IDs

The ARM captures the following transaction information from EFT, which can appear in reports:

Actions (server event actions)

ResultID	Description	Result Const
-1	If the Event Action is in progress	empty
0	If the Event Action is successfully executed	EAR_SUCCESS
1	If the Event Action fails	EAR_FAIL
2	If **STOP Processing this rule** is selected as Action.	EAR_STOP_RULE
4	If **STOP processing more rules** is selected as Action	EAR_STOP_ALL

Stop processing this rule and **Stop processing more rules** can be combined, in which case the value is the sum of the two individual values, that is, 6.

SocketConnection

ResultID	Description	Result Const
0	When socket successfully created	ER_NONE
8	Per Site socket connection limit exceeded	ER_CONNECT_FAILED_TOO_MANY_CONNECTIONS_PER_SITE
9	Max connections per IP address limit exceeded	ER_CONNECT_FAILED_TOO_MANY_CONNECTIONS_PER_IP
10	EFT denied the connection because the IP address was in the ban list or it is a remote IP address and EFT is in developer mode	ER_CONNECT_FAILED_RESTRICTED_IP
11	EFT denied the connection (failed) and added the IP address to the auto-ban list	ER_CONNECT_FAILED_BANNED_IP
12	EFT in developer mode	
13	Internal server error	

Authentications

ResultID	Description	Result Const
0	Authentication successful	LR_OK
1	Incorrect password	LR_PASSWORD_NOT_ACCEPTED
2	If user account is disabled	LR_ACCOUNT_DISABLED
3	Max connections per Site limit exceeded	LR_TOO_MANY_CONNECTIONS_PER_SITE
4	Max connections per user limit exceeded	LR_TOO_MANY_CONNECTIONS_PER_ USER
5	User per- IP address connection limit exceeded	LR_TOO_MANY_CONNECTIONS_PER_IP
6	If given protocol is not supported	LR_PROTOCOL_NOT_SUPPORTED
7	Connection on restricted IP address	LR_RESTRICTED_IP
8	If service is unavailable	LR_SERVICE_UNAVAILABLE
9	User is locked out	LR_ACCOUNT_LOCKED
10	Multi-factor authentication challenge	LR_ACCESS_CHALLENGE
11	MFA authentication required	LR_MFA_REQUIRED

ClientOperations (client transfers)

ResultID	Description	Result Const
1	If copy/move/download operation is successful	TRUE
0	If copy/move/download operation fails	FALSE

CustomCommands

ResultID	Description	Result Const
0	Command executed successfully	CER_OK
1	Command executed with socket output	CER_SYNC
2	Access is denied	CER_ACCESS_DENIED
3	Command is not found	CER_COMMAND_NOT_FOUND
4	Could not launch the selected process	CER_PROCESS_FAILED
5	Command is disabled	CER_COMMAND_DISABLED
6	Errors in parameters passed to the custom command	CER_ERROR_IN_PARAMS

ProtocolCommands

ProtocolCommands are the same as FTP result codes. Below is a brief general description.

ResultID	Description
1*xx*	Expected another reply before proceeding with a new command
2*xx*	Requested action completed successfully
3*xx*	On hold pending receipt of further information
4*xx*	Temporary failure
5*xx*	Permanent failure

Auditing Database Errors and Logging

EFT detects errors that occur while trying to connect to the ARM database and can detect errors returned from the database while attempting to perform transactions. If an error is detected while connecting to the database or when performing a transaction on the database (SQL INSERT, UPDATE, etc.) you can configure EFT to log the error to a file and to send a notification to a specified email address.

By default, database errors are logged to **\Logs**in the format *EFT_ARM_<YYYY_MM_DD_HH_MM_SS>.sql*. (By default, **C:\ProgramData\Globalscape\EFT Server\Logs**.) You can specify a different path or choose not to log the errors to a file.

For details of the **Log Settings** area, refer to Log Format, Type, and Location.

EFT also generates a Windows Event Log entry when there is an ARM database error. The log entry indicates whether auditing has stopped or if the auditing data is being stored to a log file.

If database access is lost because of a connection error or transaction error (INSERT or UPDATE), resumption of auditing to the database requires a restart of EFT or a RECONNECT request by the administrator. If EFT is configured to stop auditing, the administrator must repair the database, and then restart EFT or use RECONNECT to resume auditing to the database.

Logging to a Text File

In the **When a database error occurs**area of the Server's **Logs** tab, you can configure EFT to log the SQL statements to a text file. EFT continues to use the text file until either EFT is restarted or until a RECONNECT request is made by the administrator. EFT then notifies you by email that the logging has been saved to the text file. You can then repair the database, resume auditing to the database, and load the recorded text file SQL statements into the database.

To ensure the completeness of the audit data, the SQL statements in the text file must be loaded into the database before executing reports over the time that SQL transactions were logged to the text file.

If you click **Reconnect** to resume auditing to the database, and EFT is recording auditing information to the text file, EFT continues to log EFT file transfers and/or user sessions that are in progress to that text file. New file transfers and new user sessions will continue to be logged in the database, but any in-process transfers/ user sessions are logged to the text file to ensure that they can be inserted and linked appropriately in the database.

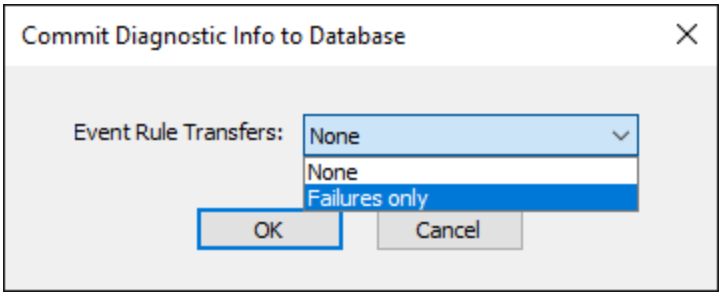
Refer to Audit Database Settings for information about configuring the connection information on EFT's **Logs** tab.

Audit Event Rule Client Outbound Transfer

You can configure whether to log no event rule transfers or event rule transfer failures.

To configure whether to log event rule transfer failures

1. On the **Server > Logs**tab, next to **Audit event rule client outbound transfer,** click **Configure**. The **Commit Diagnostic Info to Database**dialog box appears.



2. Next to **Event Rule Transfers**, click the drop-down list and click **Failures only**.
3. Click **OK**.
4. Click **Apply** on the tab to save the setting.

ARM Database Schema Change Tracking

The ARM database schema may undergo many changes between versions. Each ARM schema version is described in Knowledgebase article #11031, from newest to oldest. The database version number appears in the installer during upgrade, and you can see what the changes were.

Security Auditing

Review the topics below for details of generating a daily PCI DSS Compliance report.

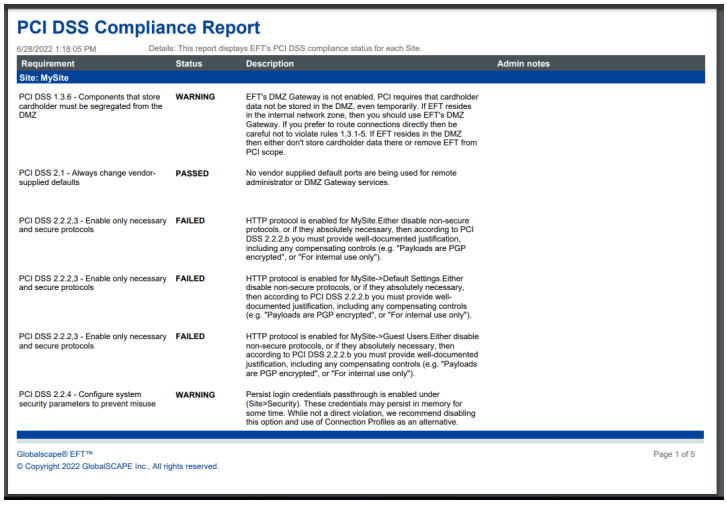
- PCI DSS Compliance Report
- Automating the PCI DSS Compliance Report
- Possible PCI DSS Compliance Report Outcomes

PCI DSS Compliance Report

The RCM module includes the ability to audit EFT for compliance with the PCI DSS requirements. EFT scans all PCI DSS requirements addressed in EFT, and then reports on the compliance status of each requirement (Pass, Fail, or Warning). The report also provides a description of the requirement tested for each item. For failed requirements, the report presents a reason the non-compliant setting was used, if you provided one at the time that particular setting was disabled/changed.

To generate the PCI DSS Compliance report

- To generate the report in real time, do one of the following:
  - On the main menu, click **Report >PCI DSS Compliance Report**. A PCI DSS Compliance report is generated for each Site.
  - In the Site's **Event Rule** node, click **Report Event**. In the right pane, click **Run Now**. The report is emailed to the email address defined in the Rule.
- To generate the report on a recurring schedule, define a Scheduler Timer Event Rule with the Generate Report Action. In the Event Rule, you can define whether to email the report and/or save the report to a file. A report is generated specific to the Site on which the Event Rule is configured.



PCI DSS Compliance Report

6/28/2022 1:18:05 PM Details: This report displays EFT's PCI DSS compliance status for each Site.

Requirement	Status	Description	Admin notes
Site: MySite			
PCI DSS 1.3.6 - Components that store cardholder must be segregated from the DMZ	**WARNING**	EFT's DMZ Gateway is not enabled. PCI requires that cardholder data not be stored in the DMZ, even temporarily. If EFT resides in the internal network zone, then you should use EFT's DMZ Gateway. If you prefer to route connections directly then be careful not to violate rules 1.3.1-5. If EFT resides in the DMZ then either don't store cardholder data there or remove EFT from PCI scope.	
PCI DSS 2.1 - Always change vendor-supplied defaults	**PASSED**	No vendor supplied default ports are being used for remote administrator or DMZ Gateway services.	
PCI DSS 2.2.2,3 - Enable only necessary and secure protocols	**FAILED**	HTTP protocol is enabled for MySite.Either disable non-secure protocols, or if they absolutely necessary, then according to PCI DSS 2.2.2.b you must provide well-documented justification, including any compensating controls (e.g. "Payloads are PGP encrypted", or "For internal use only").	
PCI DSS 2.2.2,3 - Enable only necessary and secure protocols	**FAILED**	HTTP protocol is enabled for MySite->Default Settings.Either disable non-secure protocols, or if they absolutely necessary, then according to PCI DSS 2.2.2.b you must provide well-documented justification, including any compensating controls (e.g. "Payloads are PGP encrypted", or "For internal use only").	
PCI DSS 2.2.2,3 - Enable only necessary and secure protocols	**FAILED**	HTTP protocol is enabled for MySite->Guest Users.Either disable non-secure protocols, or if they absolutely necessary, then according to PCI DSS 2.2.2.b you must provide well-documented justification, including any compensating controls (e.g. "Payloads are PGP encrypted", or "For internal use only").	
PCI DSS 2.2.4 - Configure system security parameters to prevent misuse	**WARNING**	Persist login credentials passthrough is enabled under (Site>Security). These credentials may persist in memory for some time. While not a direct violation, we recommend disabling this option and use of Connection Profiles as an alternative.	

Globalscape® EFT™ Page 1 of 5

© Copyright 2022 GlobalSCAPE Inc., All rights reserved.

For a description of each PCI DSS requirement covered in the report, refer to How PCI DSS Requirements Addressed.

For details of generating reports, refer to Generating a Report.

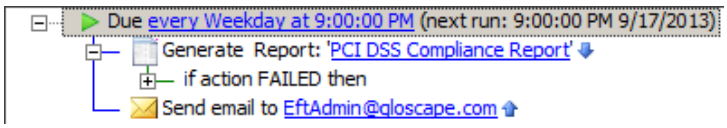
Related Topics

- Warnings for HS Violations
- PCI DSS Requirements

- Possible PCI DSS Compliance Report Outcomes
- Introduction to Event Rules
- Defining Event Rules
- Scheduler (Timer) Event
- Generate Report Action

Automating the Compliance Report

When you create a high security-enabled Site, EFT creates a Report Event Rule automatically. The **Report Event** Rule generates a PCI DSS Compliance Report once per week using the Generate Report Action. The report is converted to HTML and then emailed using the Send notification email Action and the %FS.REPORT_CONTENT% variable. You can edit the Rule to specify when to generate the report and to whom to send the report.



Optionally, you can run the PCI DSS Compliance Report "on the fly" by clicking **Reports > Run PCI DSS Compliance Report** on the administration interface main menu. If the Regulatory Compliance Module (RCM) is not activated, the PC DSS Compliance Report is not available.

PCI DSS Possible Compliance Report Outcomes

The PCI DSS Compliance Report displays the requirement name, status (PASSED, FAILED, WARNING), description of the requirement, notes that you typed in the Warning box (explanation, justification, or compensating control), report name, and date the report was generated, and description of the report. The report is grouped by and sorted by PCI DSS Requirement.

If the report is generated after the trial has expired, the report contains a statement stating that the module has expired instead of the standard report.

When in trial or after the module is activate, the report contains the following information:

The status of audited PCI DSS requirements appears in the report.

- 1.x – DMZ Gateway disabled or no connectivity
- 2.x – Remote administrator enabled by not secure, vendor defaults in use, insecure protocols in use (FTP, HTTP) or insecure settings (NOOP and FXP), auto-ban/flood detection set too low or disabled, and login credential persistence enabled.
- 3.x – Disk quotas not present for limiting storage amounts, missing clean-up rule for data retention and disposal compliance.
- 4.x – Weak cryptography in use (SSL version, cipher strength, manually specified ciphers, weak HMACs), insecure settings such as SSL clear command clear data channel in use.
- 5.x – No checks
- 6.x – No checks
- 7.x – Presence of more than one full-control administrator account
- 8.x – Password length or complexity not enforced, password reuse allowed, idle session timeout disabled or set to high, inactive accounts not disabled or removed after 90 days, failed logins not resulting in account lockout after six (or less) attempts, password reset not allowed, password reset not forced on initial login, anonymous accounts present, and passwords not expiring after 90 days or sooner.
- 9.x – Secure wiping of deleted data not enabled
- 10.x – ARM not enabled or no connectivity

- 11.x – No checks
- 12.x – No checks

Refer to How EFT Addresses PCI DSS Requirements for details of each requirement.

Reporting

(Requires the Auditing and Reporting module to be licensed.) The Auditing and Reporting module provides numerous predefined reports which you can use as is, edit to your needs, or use as templates to create new reports. You can also define custom reports using the built-in Report Designer.

- Descriptions of Preconfigured Reports
- Generating a Report
- Using Report Filters
- Defining Custom Reports
- Managing Reports

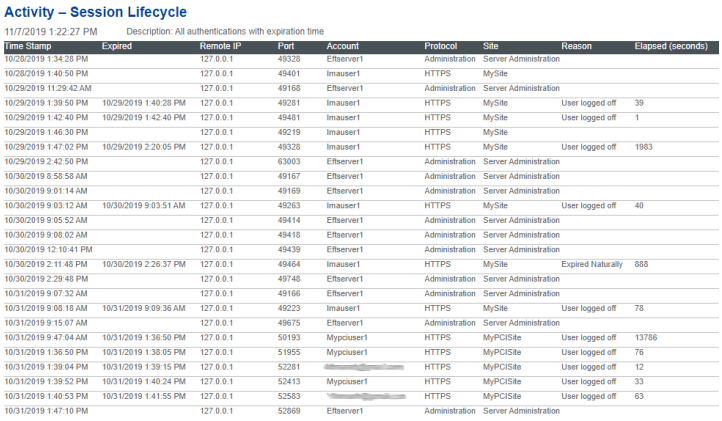
Descriptions of Preconfigured Reports

The Auditing and Reporting module comes with a number of preconfigured reports that allow you to start analyzing data right away. The report templates are **.xml** files and are installed in **%systemdrive%\ProgramData\Globalscape\EFT Server\Reports** or **\EFT Server\Reports**. If you plan to edit the default templates, it is a good idea to save a backup of them first. You can use these reports as is, or as templates to create your own custom reports.

The preconfigured reports described below are provided with the Auditing and Reporting module. You can run the reports as is or edit them to suit your specific needs.

- **Activity - AS2 Transfers (Detailed)** - A verbose AS2 file transfer report that provides the information necessary for troubleshooting problem transactions.
- **Activity - AS2 Transfers (Summary) -** A transaction report that displays the same information as shown on the Transfers - AS2 node. The report queries all AS2 transactions for the dates specified, grouped by site, sorted by date, and listed in reverse chronological order.
- **Activity - by Permissions Group** - This report displays the various Actions performed by all the groups, such as administrator, All users, and Guests, and it displays Date/Time, Remote IP address, protocol, Action, filename, folder, KB transferred, and the result.
- **Activity - by Users (Detailed) -** This report displays all folders and files created and the delete activity for all users who logged on to EFT during a particular period, grouped by username, and sorted in reverse chronological order. The report includes the time stamp, remote IP address of the user, protocol, Action, file name, folder, KB transferred, and the result.
- **Activity - by Users (Summary)** - This report displays the transfer activity (total number of uploads and downloads) for all users who logged on to EFT during the date range specified, grouped by username, subgrouped by date, sorted by username, then transfer direction, and date, in ascending order.
- **Activity - File Scanned Data Results** - This report displays all scanned data results.
- **Activity - File Transfers as Client -** This report displays all file transfers initiated by EFT.
- **Activity - File Transfers as Server** - This report displays all transfers initiated by remote clients.

- **Activity - Session Lifecycle** - This report displays authentications and session expired time. (NOTE: If an EFT user connects to EFT using CuteFTP over HTTPS and uploads several files, the report does not include data in the Expired (logout time), Reason, or Elapsed columns.)

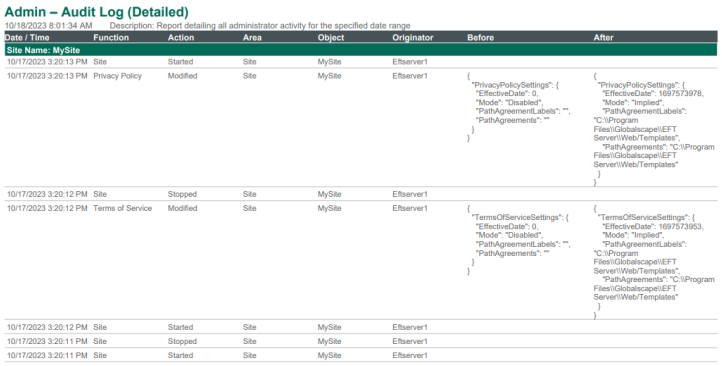


Activity – Session Lifecycle

11/7/2019 1:22:27 PM Description: All authentications with expiration time

Time Stamp	Expired	Remote IP	Port	Account	Protocol	Site	Reason	Elapsed (seconds)
10/28/2019 1:34:28 PM		127.0.0.1	49328	Eftserver1	Administration	Server Administration		
10/28/2019 1:40:50 PM		127.0.0.1	49401	Imauser1	HTTPS	MySite		
10/29/2019 11:29:42 AM		127.0.0.1	49168	Eftserver1	Administration	Server Administration		
10/29/2019 1:39:50 PM	10/29/2019 1:40:28 PM	127.0.0.1	49281	Imauser1	HTTPS	MySite	User logged off	39
10/29/2019 1:42:40 PM	10/29/2019 1:42:40 PM	127.0.0.1	49481	Imauser1	HTTPS	MySite	User logged off	1
10/29/2019 1:46:30 PM		127.0.0.1	49219	Imauser1	HTTPS	MySite		
10/29/2019 1:47:02 PM	10/29/2019 2:20:05 PM	127.0.0.1	49328	Imauser1	HTTPS	MySite	User logged off	1983
10/29/2019 2:42:50 PM		127.0.0.1	63003	Eftserver1	Administration	Server Administration		
10/30/2019 8:58:58 AM		127.0.0.1	49167	Eftserver1	Administration	Server Administration		
10/30/2019 9:01:14 AM		127.0.0.1	49169	Eftserver1	Administration	Server Administration		
10/30/2019 9:03:12 AM	10/30/2019 9:03:51 AM	127.0.0.1	49263	Imauser1	HTTPS	MySite	User logged off	40
10/30/2019 9:05:52 AM		127.0.0.1	49414	Eftserver1	Administration	Server Administration		
10/30/2019 9:08:02 AM		127.0.0.1	49418	Eftserver1	Administration	Server Administration		
10/30/2019 12:10:41 PM		127.0.0.1	49439	Eftserver1	Administration	Server Administration		
10/30/2019 2:11:48 PM	10/30/2019 2:26:37 PM	127.0.0.1	49464	Imauser1	HTTPS	MySite	Expired Naturally	888
10/30/2019 2:29:48 PM		127.0.0.1	49748	Eftserver1	Administration	Server Administration		
10/31/2019 9:07:32 AM		127.0.0.1	49166	Eftserver1	Administration	Server Administration		
10/31/2019 9:08:18 AM	10/31/2019 9:09:36 AM	127.0.0.1	49223	Imauser1	HTTPS	MySite	User logged off	78
10/31/2019 9:15:07 AM		127.0.0.1	49675	Eftserver1	Administration	Server Administration		
10/31/2019 9:47:04 AM	10/31/2019 1:36:50 PM	127.0.0.1	50193	Mypciuser1	HTTPS	MyPCISite	User logged off	13786
10/31/2019 1:36:50 PM	10/31/2019 1:38:05 PM	127.0.0.1	51955	Mypciuser1	HTTPS	MyPCISite	User logged off	76
10/31/2019 1:39:04 PM	10/31/2019 1:39:15 PM	127.0.0.1	52281	[redacted]	HTTPS	MyPCISite	User logged off	12
10/31/2019 1:39:52 PM	10/31/2019 1:40:24 PM	127.0.0.1	52413	Mypciuser1	HTTPS	MyPCISite	User logged off	33
10/31/2019 1:40:53 PM	10/31/2019 1:41:55 PM	127.0.0.1	52583	[redacted]	HTTPS	MyPCISite	User logged off	63
10/31/2019 1:47:10 PM		127.0.0.1	52869	Eftserver1	Administration	Server Administration		

- **Admin Activity - Upload Quota Usage** - This report is available only when adding the System - Report Action to the File Uploaded Event in Event Rules. This report displays upload quota usage, monthly, grouped by site name, sub-grouped by the folder.
- **Admin - Audit Log** - This report displays a summary of all EFT administrator activity for the specified date range.
- **Admin - Audit Log (Detailed)** - This report displays all EFT administrator activity for the specified data range, with Before and After details.



Admin – Audit Log (Detailed)

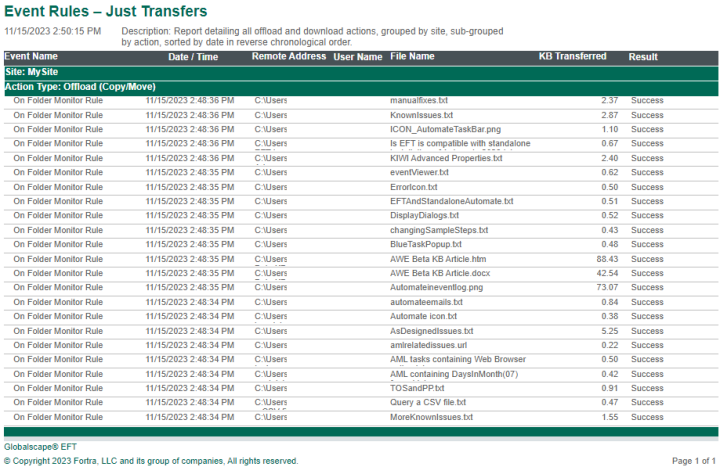
10/18/2023 8:01:34 AM Description: Report detailing all administrator activity for the specified date range

Date / Time	Function	Action	Area	Object	Originator	Before	After
Site Name: MySite							
10/17/2023 3:20:13 PM	Site	Started	Site	MySite	Eftserver1		
10/17/2023 3:20:13 PM	Privacy Policy	Modified	Site	MySite	Eftserver1	{ "PrivacyPolicySettings": { "EffectiveDate": 0, "Mode": "Disabled", "PathAgreementLabels": "", "PathAgreements": "" } }	{ "PrivacyPolicySettings": { "EffectiveDate": 1697573978, "Mode": "Implied", "PathAgreementLabels": "C:\\Program Files\\Globalscape\\EFT Server\\Web/Templates", "PathAgreements": "C:\\Program Files\\Globalscape\\EFT Server\\Web/Templates" } }
10/17/2023 3:20:12 PM	Site	Stopped	Site	MySite	Eftserver1		
10/17/2023 3:20:12 PM	Terms of Service	Modified	Site	MySite	Eftserver1	{ "TermsOfServiceSettings": { "EffectiveDate": 0, "Mode": "Disabled", "PathAgreementLabels": "", "PathAgreements": "" } }	{ "TermsOfServiceSettings": { "EffectiveDate": 1697573953, "Mode": "Implied", "PathAgreementLabels": "C:\\Program Files\\Globalscape\\EFT Server\\Web/Templates", "PathAgreements": "C:\\Program Files\\Globalscape\\EFT Server\\Web/Templates" } }
10/17/2023 3:20:12 PM	Site	Started	Site	MySite	Eftserver1		
10/17/2023 3:20:11 PM	Site	Stopped	Site	MySite	Eftserver1		
10/17/2023 3:20:11 PM	Site	Started	Site	MySite	Eftserver1		

- **Admin - Authentications -** This report shows administrator connections (success and failures) to the this EFT for the give date range.
- **Content Integrity Control** - A report showing all Event Rules with CIC actions, grouped by site name, sub-grouped by the user-defined event name, sorted by the unique event ID (not shown) in descending order. Includes Parameters, Begin and End Date\ Time, and Result.

- **Event Rules - by Trigger Name (Summary)** - This report summarizes all Event Rules with their corresponding Actions, grouped by Site name, subgrouped by the user-defined Event name, sorted by the unique Event ID (not shown in report) in descending order.
- **Event Rules - by Trigger Type (Detailed)** - This report displays the Event Rule activity by user-defined Event name, grouped by Site name, subgrouped by the Event type, sorted by date in reverse chronological order.
- **Event Rules - by Trigger Type (Summary)** - This report summarizes the Event Rule activity by user-defined Event name, grouped by Site name, sub-grouped by the Event type, sorted by date in reverse chronological order.

- **Event Rules - Just Transfers** - This report details all offload and download Actions, grouped by Site subgrouped by Action, sorted by date in reverse chronological order.



Event Rules – Just Transfers

11/15/2023 2:50:15 PM Description: Report detailing all offload and download actions, grouped by site, sub-grouped by action, sorted by date in reverse chronological order.

Event Name	Date / Time	Remote Address	User Name	File Name	KB Transferred	Result
Site: MySite						
Action Type: Offload (Copy/Move)						
On Folder Monitor Rule	11/15/2023 2:48:36 PM	C:\Users		manualfixes.txt	2.37	Success
On Folder Monitor Rule	11/15/2023 2:48:36 PM	C:\Users		KnownIssues.txt	2.87	Success
On Folder Monitor Rule	11/15/2023 2:48:36 PM	C:\Users		ICON_AutomateTaskBar.png	1.10	Success
On Folder Monitor Rule	11/15/2023 2:48:36 PM	C:\Users		Is EFT is compatible with standalone	0.67	Success
On Folder Monitor Rule	11/15/2023 2:48:36 PM	C:\Users		KIWI Advanced Properties.txt	2.40	Success
On Folder Monitor Rule	11/15/2023 2:48:35 PM	C:\Users		eventViewer.txt	0.62	Success
On Folder Monitor Rule	11/15/2023 2:48:35 PM	C:\Users		ErrorIcon.txt	0.50	Success
On Folder Monitor Rule	11/15/2023 2:48:35 PM	C:\Users		EFTAndStandaloneAutomate.txt	0.51	Success
On Folder Monitor Rule	11/15/2023 2:48:35 PM	C:\Users		DisplayDialogs.txt	0.52	Success
On Folder Monitor Rule	11/15/2023 2:48:35 PM	C:\Users		changingSampleSteps.txt	0.43	Success
On Folder Monitor Rule	11/15/2023 2:48:35 PM	C:\Users		BlueTaskPopup.txt	0.48	Success
On Folder Monitor Rule	11/15/2023 2:48:35 PM	C:\Users		AWE Beta KB Article.htm	88.43	Success
On Folder Monitor Rule	11/15/2023 2:48:35 PM	C:\Users		AWE Beta KB Article.docx	42.54	Success
On Folder Monitor Rule	11/15/2023 2:48:35 PM	C:\Users		Automateineventlog.png	73.07	Success
On Folder Monitor Rule	11/15/2023 2:48:34 PM	C:\Users		automateemails.txt	0.84	Success
On Folder Monitor Rule	11/15/2023 2:48:34 PM	C:\Users		Automate icon.txt	0.38	Success
On Folder Monitor Rule	11/15/2023 2:48:34 PM	C:\Users		AsDesignedIssues.txt	5.25	Success
On Folder Monitor Rule	11/15/2023 2:48:34 PM	C:\Users		amlrelatedissues.url	0.22	Success
On Folder Monitor Rule	11/15/2023 2:48:34 PM	C:\Users		AML tasks containing Web Browser	0.50	Success
On Folder Monitor Rule	11/15/2023 2:48:34 PM	C:\Users		AML containing DaysInMonth(07)	0.42	Success
On Folder Monitor Rule	11/15/2023 2:48:34 PM	C:\Users		TOSandPP.txt	0.91	Success
On Folder Monitor Rule	11/15/2023 2:48:34 PM	C:\Users		Query a CSV file.txt	0.47	Success
On Folder Monitor Rule	11/15/2023 2:48:34 PM	C:\Users		MoreKnownIssues.txt	1.55	Success

Globalscape® EFT

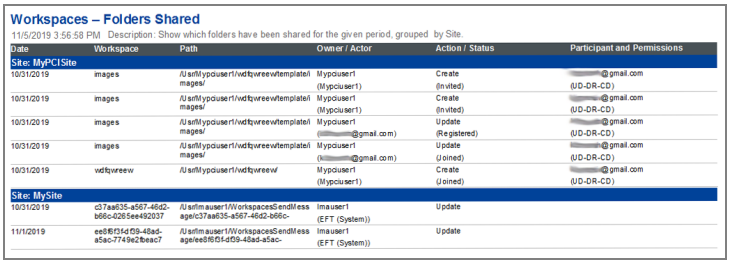
© Copyright 2023 Fortra, LLC and its group of companies, All rights reserved.

Page 1 of 1

- **Executive Summary Report** - This report summarizes the following information for the period specified:
  - Average transfer speed
  - Total number of downloads, uploads
  - Total bytes transferred (inbound/ outbound)
  - Top 5 users (by # of connections)
  - Top 5 users (by bytes transferred)
- **PCI DSS Compliance** - This report displays EFT's PCI DSS compliance status for each Site.
- **Privacy - Admin Changes to Personal Data** - This report details changes to personal data fields, organized by date/ time, Site, Template, Account, Field changed, and Before and After changes.
- **Privacy - Terms and EU Status Changes** - This report details privacy terms and EU status changes organized by date/ time, Site, Template, Account, IP address, Right Exercised, and Reason a user exercised their privacy rights.
- **Privacy - User Rights Exercised** - This report details date/ time, Site, Template, Account, IP address, Right Exercised, and Reason a user exercised their privacy rights.(See examples in Privacy Reports.)
- **Traffic - Average Transfer Rates by User** - This report displays the average transfer rate for specific users, grouped by username, subgrouped by date, sorted by username, transfer direction, and date, in descending order.
- **Traffic - Connections Summary** - This report details connections to EFT (IP address or user connections) and bytes transferred by date, grouped by Site name, sorted by date in reverse chronological order.

- **Traffic - Datewise - hourly Bytes Transferred** - This report details the connections and bytes transferred sorted by date and hour, in chronological order.
- **Traffic - Datewise - IPwise bytes transferred** - This report displays the connections established by remote IP addresses and total bytes transferred.
- **Traffic - IPwise Connections (Summary)** - This report displays the connections established by remote IP addresses and total bytes transferred.
- **Traffic - Monthwise-IPwise Bytes transferred** - This report displays the connections established by various remote IP addresses each month. It displays the Site name, month name, remote IP address, connections, and total bytes transferred.
- **Traffic - Most Active IP - Connections** - This report displays the most active IP addresses; that is, the IP addresses of the users who frequently log on to EFT. It displays the data transferred, Site name, remote IP address, and bytes transferred. This report can be used to determine Denial of Service (DoS) attacks against EFT.
- **Traffic - Most Active IP - Data Transferred** - This report displays the IP addresses of users who log on to EFT frequently; the number of connections established by various users. It displays the information on the total bytes transferred, number of connections, remote IP address, and Site name.
- **Traffic - Most Active Users - Connections** - This report displays the connections established by the most active users.
- **Traffic - Most Active Users - Data Transferred** - This report displays the usernames of users who log on to EFT frequently, the number of connections established by various users, and number of bytes transferred.
- **Traffic - Protocolwise Connections (Summary)** - This report displays the connections established by various users and the protocol used by the users to transfer the data, that is, whether the users have used FTP, HTTP, or any other protocol to upload or download the files.
- **Traffic - Sitewise - Hourly by User** - This report displays the total number of connection established by various users on a particular Site each hour.
- **Troubleshooting - Event Rules Failures** - This report displays failures related to the Event Rules.
- **Troubleshooting - Failed Logins** - This report displays failures related to logins.
- **Troubleshooting - Most Prolific Users -** This report details users with the most log on attempts.
- **Troubleshooting - Negotiated SSH Ciphers** - This report lists all negotiated SSH Ciphers organized by Time Stamp, Key Algorithm, Cipher, KEX, MAC, Compress Directory, Account, and Fingerprint (fingerprint is NULL for inbound connections).

- **Troubleshooting - Negotiated SSH Ciphers (Summary)** - This report provides a summary of negotiated SSH Ciphers
- **Troubleshooting - Negotiated SSL Ciphers** - This report list all negotiated SSL Ciphers, organized by Time Stamp, Protocol version, EncryptionCipher, KEX, Authentication, MAC, Directory Account
- **Troubleshooting - Negotiated SSL Ciphers (Summary)** - This report a summary of SSL Ciphers used, organized by Protocol version, EncryptionCipher, KEX, Authentication, MAC, Directory, Account, Count
- **Troubleshooting - Operation Errors** - This report displays protocol error codes and corresponding commands, sorted in reverse chronological order. The report includes the date and time the error occurred, remote IP address, protocol used, username, command, filename, virtual folder, and result (for example, transfer completed).
- **Troubleshooting - Socket Connection Errors(Inbound)** - This report displays the number of connection errors occurred while connecting to a site. (Refer to Winsock Error Codes for a list of Socket ID error codes.)
- **Troubleshooting - Socket Connection Errors Summary (Inbound)** - This report displays a summary of the number of connection errors occurred while connecting to a site.
- **Web Service- Invoke Event Rules (Detailed)** - This report is used to view activity for invoking Event Rules through Web Service, grouped by username, and sorted by date in reverse chronological order.
- **Workspaces Files Picked Up** - Shows shared Workspace files picked up, organized by Send Date, Sender Email, Recipient Email, File Name, File Size (KB), Subject, and Expires date.
- **Workspaces - Files Sent** - This report lists Workspace files sent, organized by Send Date, Sender Email, Recipient Email, File Name, File Size (KB), Subject, and Expires date.
- **Workspaces - Folders Shared** - This report shows which folders have been shared for the given period, grouped by Site, organized by Date, Workspace, Path, Owner/Actor, Action/Status, and Participant/Permissions.



Workspaces – Folders Shared

11/5/2019 3:56:58 PM Description: Show which folders have been shared for the given period, grouped by Site.

Date	Workspace	Path	Owner / Actor	Action / Status	Participant and Permissions
Site: MyPCISite					
10/31/2019	images	/Usr/Mypciuser1/wdfqwreewt/templates/images/	Mypciuser1 (Mypciuser1)	Create (Invited)	[redacted]@gmail.com (UD-DR-CD)
10/31/2019	images	/Usr/Mypciuser1/wdfqwreewt/templates/images/	Mypciuser1 (Mypciuser1)	Create (Invited)	[redacted]@gmail.com (UD-DR-CD)
10/31/2019	images	/Usr/Mypciuser1/wdfqwreewt/templates/images/	Mypciuser1 ([redacted]@gmail.com)	Update (Registered)	[redacted]@gmail.com (UD-DR-CD)
10/31/2019	images	/Usr/Mypciuser1/wdfqwreewt/templates/images/	Mypciuser1 ([redacted]@gmail.com)	Update (Joined)	[redacted]@gmail.com (UD-DR-CD)
10/31/2019	wdfqwreew	/Usr/Mypciuser1/wdfqwreew	Mypciuser1 (Mypciuser1)	Create (Joined)	[redacted]@gmail.com (UD-DR-CD)
Site: MySite					
10/31/2019	c37aa635-a567-46d2-b66c-0265ee492037	/Usr/fmauser1/WorkspacesSendMessage/c37aa635-a567-46d2-b66c-	fmauser1 (EFT (System))	Update	
11/1/2019	ee8f6f3f4d59-48ad-a5ac-7749e2fbeac7	/Usr/fmauser1/WorkspacesSendMessage/ee8f6f3f4d59-48ad-a5ac-	fmauser1 (EFT (System))	Update	

- **Workspaces - Folders Unshared** - This reports shows which folder shares of expired naturally or by their owner, organized by Date, Workspace, Path, Owner or Actor, Status, and Participant(s).

Generating a Report

The ARM comes with a number of preconfigured reports to help you start analyzing data right away. The built-in reports were designed to respond to the most common data analysis requests. Refer to Preconfigured Reports for a list of available reports. If you are using SQL Express as your database, you may not be able to generate a report remotely, unless the connecting account is a trusted SQL Server connection (that is, if SQL Server and the remote computer are in the same domain, or if SQL Server is configured to allow "mixed authentication.")

To generate a report

1. In the administration interface, connect to EFT and the reports database, and then click the **Reports**tab.
2. In the left pane, click the desired report.
3. In the right pane, in the **Report Filters** boxes, specify any filters.
4. Specify a date range from which you want pull data.
5. Click **Show Report**. The ARM connects to the auditing database and displays the data in a PDF viewer. ARM displays the first page of the report as soon as the data is ready, then continues to load additional pages. If you want to stop a report from loading, click another report in the left pane.

   Generated report files can be found in **..\ProgramData\Globalscape\EFT Server\GeneratedReports**. The automatically generated PCI DSS report is saved as both HTML and PDF.

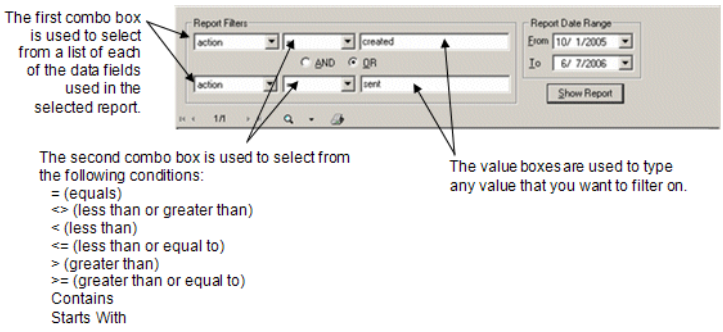
Related Topics

- Descriptions of Preconfigured Reports
- Filtering a Report
- Custom Reports
- Managing Reports

Using Report Filters

You can filter the fields in a report based on various conditions to display only the data that meet the filtering criteria.

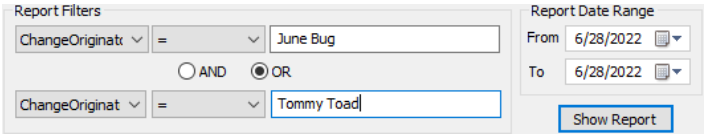
The **Report Filters** area contains two sets of combo boxes, operands (AND, OR), and a text box.



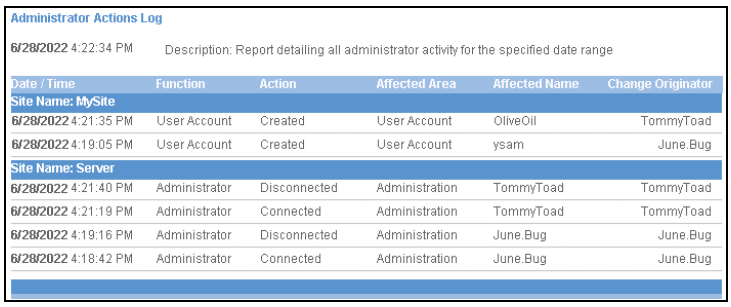
Use the second set of filters to further define the report using **AND** or **OR**.

For example, to show only changes made by TommyToad and June.Bug, set the following filters:

1. In the first combo box, click **Change Originator**.
2. In the second combo box, click the equals sign (**=**).
3. Type `June Bug` in the text box.
4. Click **OR**.
5. In the bottom filter, click **Change Originator**, equals, and type `Tommy Toad`.



6. Specify a date range, and then click **Show Report**.
7. The report now displays only changes made by administrators TommyToad or June.Bug.



Administrator Actions Log

6/28/2022 4:22:34 PM Description: Report detailing all administrator activity for the specified date range

Date / Time	Function	Action	Affected Area	Affected Name	Change Originator
Site Name: MySite					
6/28/2022 4:21:35 PM	User Account	Created	User Account	OliveOil	TommyToad
6/28/2022 4:19:05 PM	User Account	Created	User Account	ysam	June.Bug
Site Name: Server					
6/28/2022 4:21:40 PM	Administrator	Disconnected	Administration	TommyToad	TommyToad
6/28/2022 4:21:19 PM	Administrator	Connected	Administration	TommyToad	TommyToad
6/28/2022 4:19:16 PM	Administrator	Disconnected	Administration	June.Bug	June.Bug
6/28/2022 4:18:42 PM	Administrator	Connected	Administration	June.Bug	June.Bug

(If you had clicked AND instead of OR, nothing would appear, because no changes can be made by two administrators at the same time.)

Defining Custom Reports

The topics below provide information regarding creating custom reports of Globalscape EFT activity in the administration interface.

- The VSReport Designer
- Opening VSReport Designer
- Creating a Report with the Report Wizard
- Creating a Report in Design Mode
- Changing Field Section and Report Properties
- Adding Editing and Deleting Fields in the Report
- Changing the Data Source
- Grouping and Sorting Data
- Example: Creating a Custom Report

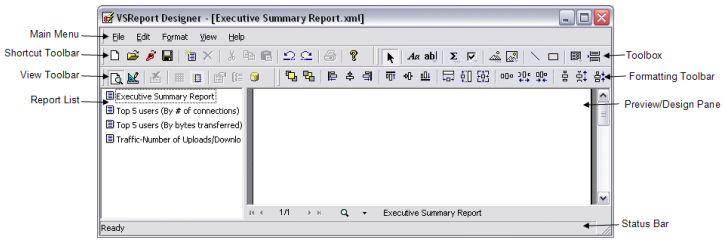
VSReport Designer

Querying, sorting, filtering, and reporting on EFT data can be accomplished by editing one of the existing reports or creating a new report in the provided report editor. This tool can be launched from within the administration interface.

The report editor tool bundled with ARM is a robust report designer licensed from Component One. During EFT evaluation period, VSReport Designer is available for use as a fully functional trial. A license for VSReport Designer is included with each purchase of ARM. After the trial, ARM must be activated along with EFT to continue using VSReport Designer. Most of the main functions of the report designer are described in this help file; however, the VSReport Designer has its own Help file, accessed by clicking **Help** on the report designer's main menu.

In VSReport Designer, you can work on existing report templates, change field locations and properties, add various levels of grouping, sorting, and so on. You can also create new reports and select ARM's database tables from which to retrieve data fields or paste in SQL code for advanced queries of the data source, giving customers complete freedom in designing their report. Styles for the report (colors, fonts, background logo images, etc.) can all be manipulated from within the designer. You can also import report definitions from Microsoft Access files (MDB, ADP) and VSReport Designer files (VSR) from within the Report Designer.

Translation of Access reports requires that Microsoft Access is installed. Once the report is imported into the Designer, Access is no longer required.



The main Designer dialog box includes the following:

- **Report list** - The left pane of the Report Designer lists all report templates contained in the current report definition file. (A report can contain multiple report templates.) You can double-click a report name to preview or edit the report. You can also right-click in the list to rename, copy, and delete report templates.
- **Preview/Design pane**- The right pane is the main working area of VSReport Designer. In preview mode, it displays the current report. In design mode, it shows the report's sections and fields and allows you to change the report definition.

- **Main Menu**- The main menu is used to access submenus, load and save report definition files, import report definitions, and print reports.

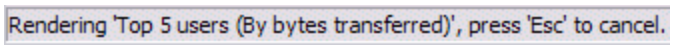
- **Shortcut toolbar**- Shortcuts are used to access the most common menu functions: new file, open, import, save, print, undo/redo, cut/copy/paste, create/delete report, and help.

- **View toolbar** - The **View** toolbar allows you to easily switch between preview and design modes, activate the design grid, and display the property and grouping panes.

- **Toolbox**- The **Toolbox** provides tools for creating report fields. This toolbar is enabled only in design mode.

- **Formatting toolbar** - The **Formatting**toolbar provides shortcuts to tools for aligning, sizing, and spacing report fields. This toolbar is enabled only in design mode.

- **Status bar** - The **Status bar** at the bottom of the Report Designer displays information about what VSReport Designer is working on (for example, loading, saving, printing, rendering, importing, etc.).



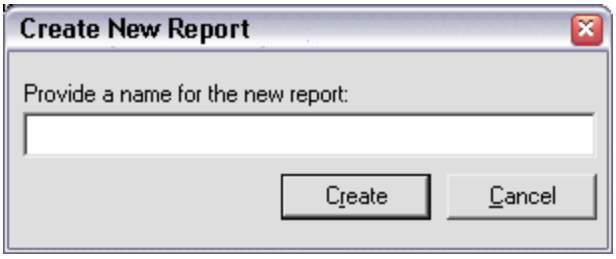
Opening VSReport Designer

When you create a new report, you create it manually or use the Report Wizard. Both methods are provided in the VSReport Designer, as described below.

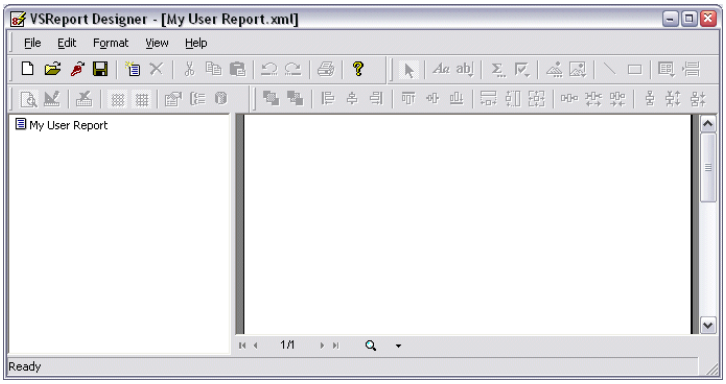
To open VSReport Designer

1. In the administration interface, connect to EFT, then do one of the following:
   - On the toolbar, click the click **New Report** icon .
   - On the main menu, click **Reports >New Report**.
   - Click the **Reports** tab, and then click the **New Report** icon at the bottom of the right pane.

   The **New Report** dialog box appears.



2. Type a title for the new report, and then click **Create**. The **Report Designer** appears.



3. Do one of the following to create a report:
    - **Manually define the report:** click the report name in the left pane, click the **Design** icon , then continue with the instructions in Using Design Mode, Changing Field, Section, and Report Properties, Changing the Data Source, Adding, Editing, and Deleting Fields in the Report, and Grouping and Sorting Data.
    - Use the Report Wizard: In the Report Designer, click **File >New Report** or click the **New Report** icon on the toolbar.

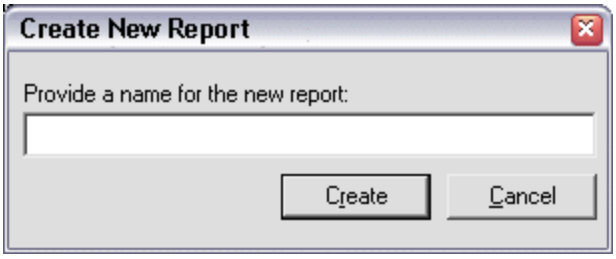
Creating a Report with the Report Wizard

The easiest way to start a new report is to use the Report Wizard. The Report Wizard will help you create a basic report, specify the data source, fields to include in the report, layout of the report, and styles or labels to use in the report.

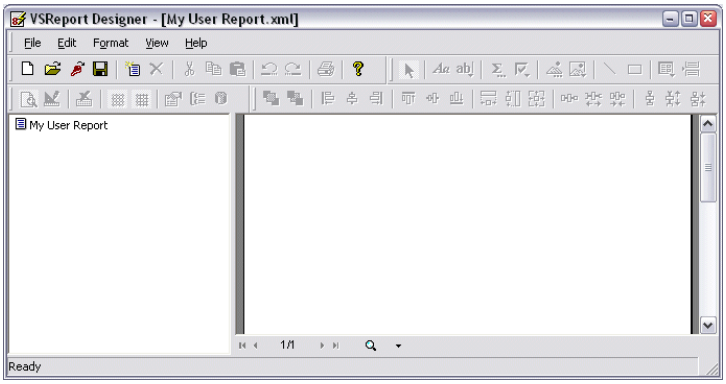
To use the Report Wizard

1. In the administration interface, connect to EFT, then do one of the following:
   - On the toolbar, click the click **New Report** icon .
   - On the main menu, click **Reports >New Report**.
   - Click the **Reports** tab, and then click the **New Reports**icon on the bottom toolbar.

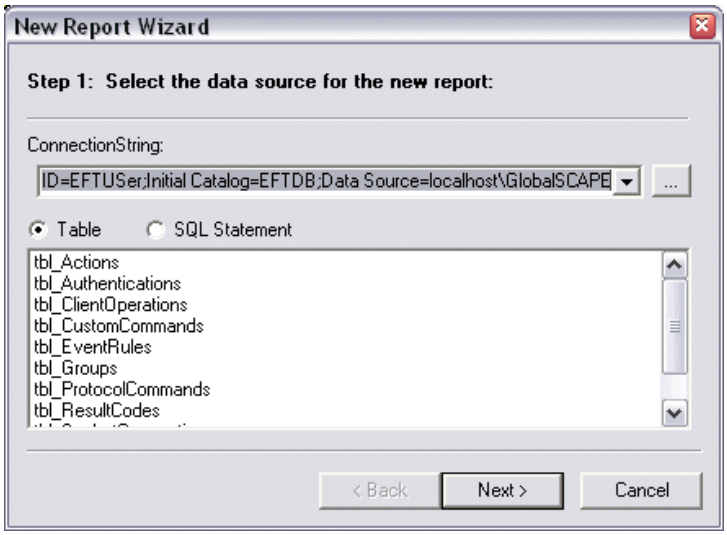
   The **New Report** dialog box appears.



2. Type a title for the new report, and then click **Create**. The **Report Designer** appears.



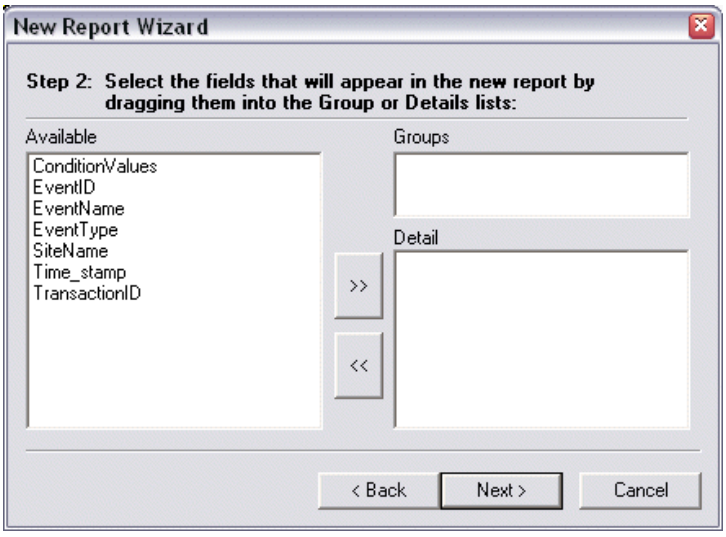
3. Click **File >New Report** or click the **New Report** icon on the toolbar. The **New Report Wizard** appears.



4. By default, the **ConnectionString** box displays information for the database that you specified when you installed the Auditing and Reporting module. Click **Next** and go to step 5 or, if necessary, you can type a different string that is used to connect to the data source.
    a. Click the ellipsis to define the connection string. The **Data Link Properties** dialog box appears.
    b. On the **Provider** tab, click **Microsoft OLE DB Provider for SQL Server** as the provider to connect to the SQL Server database, and then click **Next**. The **Connection** tab appears.
    c. In **Select or enter a server name**, click the arrow to select a name or type the name of EFT.
    d. In **Enter information to log on to EFT**, click an authentication option to log on to EFT:
        - **Use Windows NT Integrated security** - Your computer automatically picks up the credentials from your computer and connects you to the database.
        - **Use a specific user name and password** - Specify the user name and the password to be used to log on to EFT. Select the **Allow saving password** check box to save the password in the connection string.

> **NOTE:** Select the **Blank password** check box if EFT requires a blank password to log on the database server. Even if you do not type a password when you create a user account on a database server, you can select the **Allow saving password** check box. In this case, EFT takes a dummy password value and saves that value in the connection string. Selecting the **Blank password** check box disables the password field.

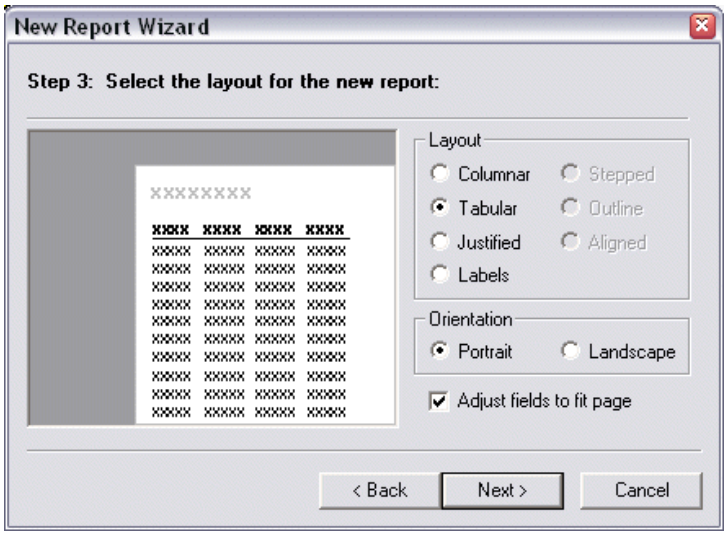
5. Click one of the following:
    - Select the database on EFT, and then click a database in the list.
    - Attach a database file as a database name - Click the ellipsis icon to browse for the SQL Server database file (*.mdf). The **Select SQL Server Database File** dialog box appears. Select a file, then click **Open**. The path to the file appears in the **Using the filename** box.
6. Click **OK** in the **Data Link Properties** dialog box to return to the **New Report Wizard**.
7. Click one of the following:
    - **Table** to select a database table, such as `tbl_EventRules`.
    - **SQL Statement** to type a SQL query in the bottom box, such as `SELECT * FROM tbl_EventRules`.
8. Click **Next**. The fields that appear in the **Available** list depend on your selection in the previous step. For example, if you selected `tbl_EventRules`, the fields for Event Rules appear.



9. Double-click a field, click it and use the arrows, or drag and drop one or more field to the **Groups** list. Group fields define how the data is sorted and summarized. The information in the **Detail** list is grouped according to the group name. The **Detail** list displays the details for each group. Detail fields define the information you want to appear in the report. For example, if you move SiteName to the **Groups** list and Time_stamp, EventName, and so on to the **Detail** list, then the report displays the time stamp and events under the respective Sites, considering different Sites as different groups.

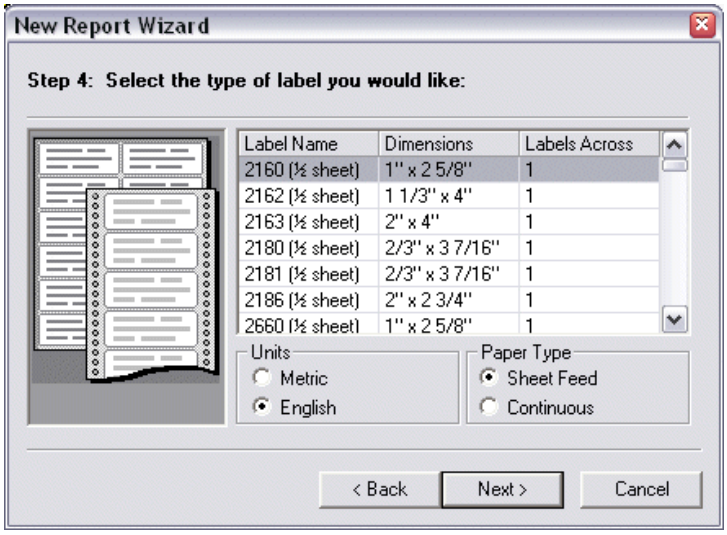
    You can also drag and drop the available fields into the Groups or Detail section.

10. Click **Next**. The layout options appear.

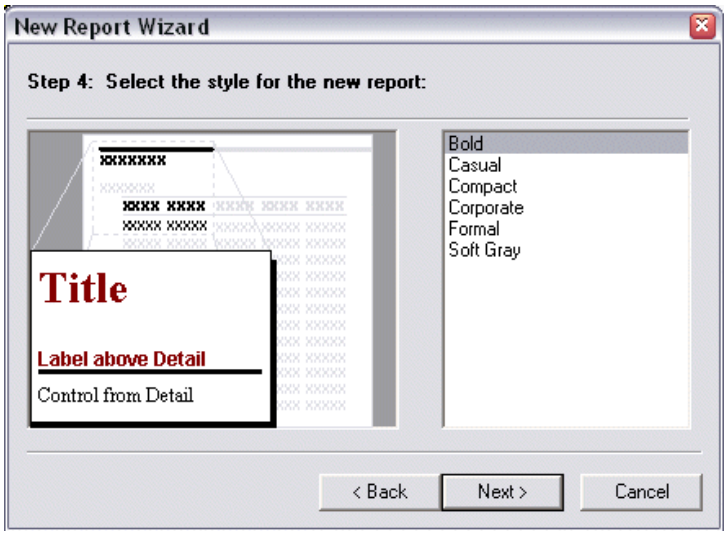


11. Click a layout for the report. When you select a layout, a thumbnail preview appears on the left to give you an idea of how the layout will appear on the page. There are two groups of layouts. The first is for the reports with no groups defined and other is for the reports with group fields defined.
    - If you did ***not*** define the Group field, the following options are available:
        - Columnar
        - Tabular
        - Justified
        - Labels. The **Labels** layout option is used to print Avery-style labels, available in a variety of sizes, blank or preprinted. If you select this option, the next page offers options for the type of label for your report.
    - If you defined the Group field, the following options are available:
        - Stepped
        - Outline
        - Aligned
    - If you selected any option other than **Labels**, click the report orientation from the following options. If you select the **Labels** option, the **Orientation** options are disabled.
        - Portrait
        - Landscape
    - Select the **Adjust fields to fit page** check box to adjust fields in a way that they fit the page.
12. Click **Next**.

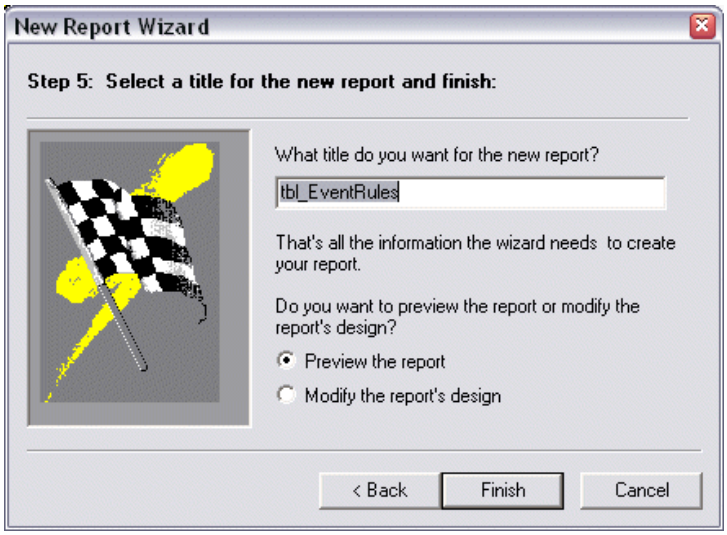
13. Do one of the following:
    - If you specified **Labels**, click a type of label in the **Labels** list, then specify the Units, **Metric** or **English**, and the paper type, **Sheet Feed** (single sheet) or **Continuous** (continuous paper).



    - If you specified anything other than **Labels**, specify a style for the report title.



14. Click **Next**. The title page of the wizard appears.



15. Type a title for the report.
16. Do one of the following:
    - To view the report, click the **Preview the report**.
    - To modify the report in Design view, click the **Modify the report's design**.
17. Click **Finish**. Your new report name appears in the left pane of the Report Designer. The right pane displays a preview of the report or the design view, depending on your selection in the previous step.
18. Click **Save** to save the report.
19. Click **File >Close** to close VSReport Designer. The report appears on the **Reports** tab.
20. Use Design mode to add/remove fields, resize fields, add graphics, and so on.

Creating a Report in Design Mode

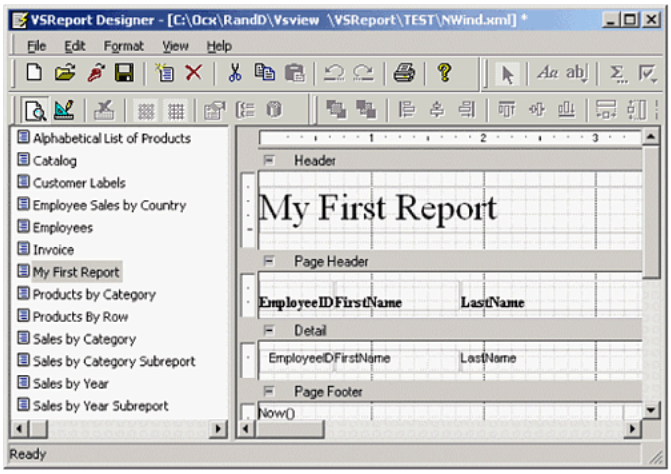
The New Report Wizard is used to specify a data source and a basic framework for the report. To get exactly the report you want, you can adjust and enhance the data fields and layout. The Report Designer provides the options to modify the report to fit your needs.

To use the Report Designer design mode

1. In the administration interface, click the **Reports**tab, then do one of the following:
   - Click the report that you want to modify, and then click **Edit Report**.
   - Create a new report. (Refer to Creating a Report with the Report Wizard for instructions.)

   The report appears in the Report Designer.
2. The left pane of the Report Designer lists all report templates contained in the current report definition file. Click the report that you want to modify, and then click the **Design** icon on the **View** toolbar, or on the main menu, click **View >Design**.

   The right pane switches from **Review** mode to **Design** mode, and displays the controls and fields that make up the report.



The Report Sections

The report is divided into sections, labeled **Header**, **Page Header**, **Detail**, and **Page Footer**, containing fields that hold the labels, variables, and expressions that you want in the generated report. The sections determine the appearance of the beginning and end of the report, and each page and group. The table below describes where each

section appears in the report and the sort of data that typically appears in each section.

Section	Appears	Typically Contains
Report Header	Once per report	The report title and summary information for the whole report
Page Header	Once per page	Labels that describe detail fields and/or page numbers
Group Header	Once per group	Fields that identify the current group and possibly aggregate values for the group (e.g. total, percentage of the grand total)
Detail	Once per record	Fields containing data from the source record set
Group Footer	Once per group	Aggregate values for the group
Page Footer	Once per page	Page number, page count, date printed, report name
Report Footer	Once per report	Summary information for the entire report

You cannot directly add and delete sections. The number of groups determines the number of sections in a report. Each report has exactly five fixed sections (Report Header/Footer, Page Header/Footer, and Detail) plus two sections per group (a Header and a Footer).

To hide sections that you do not want to display

1. Right-click the field, click **Properties**. The **Field Properties** dialog box appears.
2. Change the property of **Visible**to **False**.

To resize a section

1. Click and hold the border of the section and drag it to the position where you want it.
   The rulers on the left and on top of the design dialog box show the size of each section (excluding the page margins). You cannot make the section smaller than the height and width required to contain the fields in it. To reduce the size of a section beyond that, move or resize the fields in the section first, then resize the section.
2. Press and hold SHIFT, and then click fields to toggle their selection status.
3. Press and hold CTRL, then drag the cursor to copy a selection.
4. Click on the corners of a field to resize it.
5. Press TAB to move the selection to the next field.

6. Press the arrow keys to move selected fields.
7. Press DELETE to remove selected fields.

If you make any mistakes while moving or editing the fields, click **Undo** and/or **Redo**.

When multiple fields are selected, you can use the buttons on the **Format** toolbar to align, resize, and space them.

You can control the design grid using the **Show Grid** and **Snap To Grid** icons.

Related Topics

- Adding, Editing, and Deleting Fields in the Report
- Changing Field, Section, and Report Properties
- Changing the Data Source
- Adding, Editing, and Deleting Fields in the Report
- Grouping and Sorting Data

Changing Field, Section, and Report Properties

You can view and edit the properties of the objects inserted in a report.

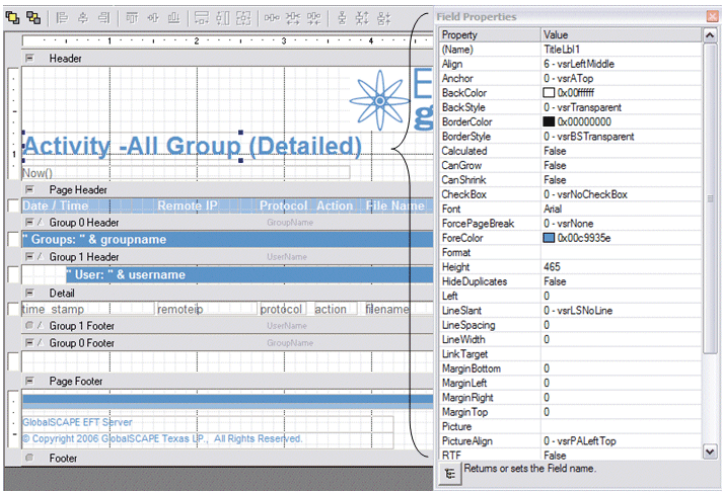
- When more than one field is selected, the **Field Properties** dialog box displays only the properties and values that all selected fields have in common and leaves the other properties blank.
- If no fields are selected and you click a section (or on the bar above a section), the selected section's properties are displayed.
- If you click the gray area in the background, the **Report** properties are displayed.

To view and edit an object's properties

- Double-click the object or select the object, then do one of the following:
  - Click **Property Window**.
  - Press F4
  - Right-click, and then click **Properties**.

  The **Field Properties** dialog box appears.

In the example below, the **Activity - All Group (Detailed)** label in the **Header** section is selected. The **Field Properties** dialog box displays the properties of the selected field.



In the **Field Properties** dialog box, you can change a property by changing its value. For example, you can change the text color by changing the **ForeColor** property. You can change the field's position and dimensions by typing new values for the **Left**, **Top**, **Width**, and **Height** properties.

The property dialog box expresses all measurements in *twips* (the native unit used by the ComponentOne report designer), but you can type in values in other units and they will be automatically converted into twips. For example, if you set the field's **Height** property to "0.5in," the property dialog box will convert it into 720 twips.

Adding, Editing, and Deleting Fields in the Report

VSReport Designer only has one type of field object; the icons in the Toolbox simply set the properties of the field to make it look and act in a certain way.

To add, edit, or delete fields in a report

1. In the Report Designer, click **View>Design** or click the **Design** icon on the toolbar. The report opens in the design mode.
2. Use the ToolBox to add fields to your report. Follow the procedures below depending on the fields that you want to add, edit, or delete.

Each icon creates a field and initializes the field's properties as follows:

Icon	Name	Description
	Label field	Creates a field that displays static text.
	Bound field	Creates a field that is bound to the source recordset. When you click this button, a menu appears and you can select the recordset field. **Bound Fields** are not limited to displaying raw data from the database. You can edit their Text property and use any VBScript expression.
	Expression Field	Creates a calculated field. When you click this button, the code editor dialog will appear so you can enter the VBScript expression whose value you want to display.
	Check box Field	Creates a bound field that displays a Boolean value as a check box. By default, the check box displays a regular check mark. You can change it into a radio button or cross mark by changing the value of the field's **Checkbox**property after it has been created.
	Unbound Picture field	Creates a field that displays a static picture, such as a logo. When you click this button, a dialog box will appear to prompt you for a picture file to insert in the report. A copy is made of the picture you select and is placed in the same directory as the report file. You must distribute this file with the application unless you embed the report file in the application. When you embed a report file in your application, any unbound picture files are embedded too.
	Bound Picture field	Creates a field that displays a picture (or object) stored in the recordset. When you click this button, a menu appears so you can select a picture field in the source recordset (if there is one; not all recordsets contain this type of field).
	Line field	Creates a line. Lines are often used as separators.
	Rectangle field	Creates a rectangle. Rectangles are often used to highlight groups of fields or to create tables and grids.
	Subreport field	Creates a field that displays another report. When you click this button, a menu appears and you can select other reports that are contained in the same report definition file.

Icon	Name	Description
	Page Break field	Creates a field that inserts a page break.

After you click any of these icons, drag the mouse over the report and the cursor will change into a crosshair. Click and drag to define a space that the new field will occupy, and then release the button to create the new field. If you change your mind, press ESC or click the arrow button to cancel the operation.

You can also add fields by copying and pasting existing fields, or by holding down the control key and dragging a field or group of fields to a new position to create a copy.

To draw a line

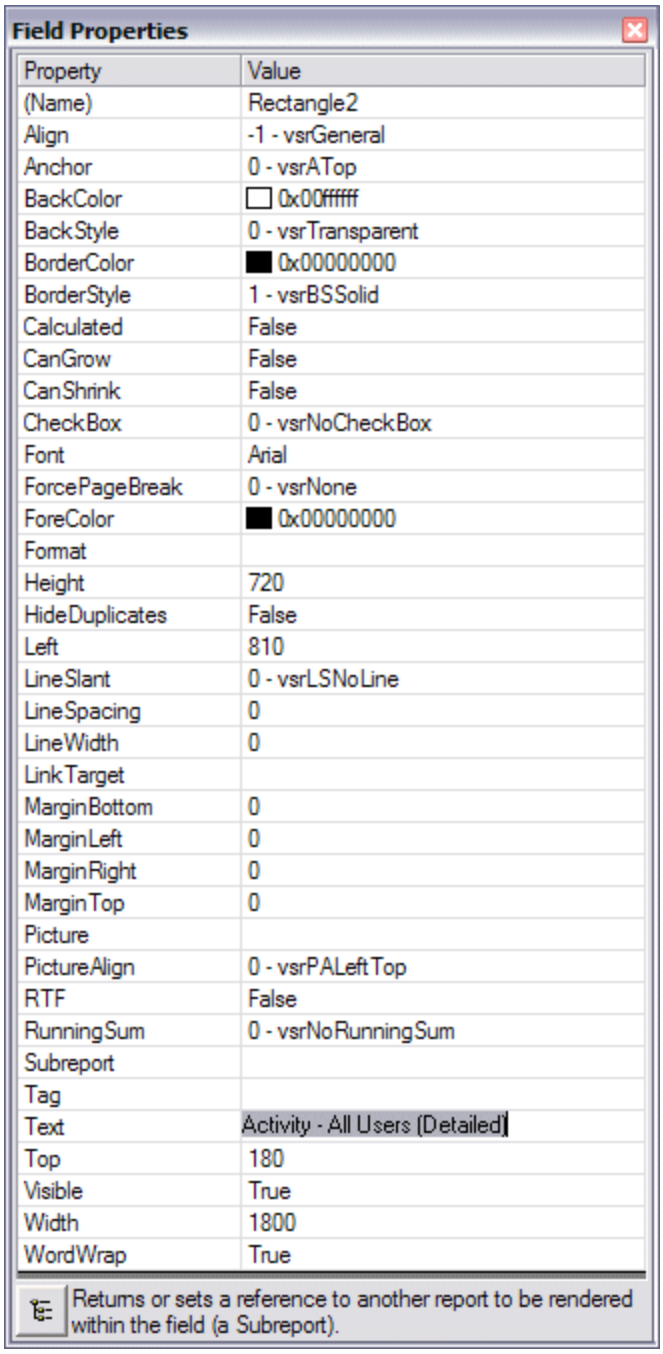
- Click **Line** , then drag the cursor where you want to draw a line.

To draw a rectangle

- Click **Rectangle** , then drag the cursor where you want to draw a rectangle.

To add or edit text

1. Insert a rectangle, or double-click or right-click an existing rectangle, and then click **Properties**. The **Field Properties** dialog box appears.



2. Scroll to **Text** in the **Property** column, click the **Value** column, then type the text; press ENTER.

To add labels

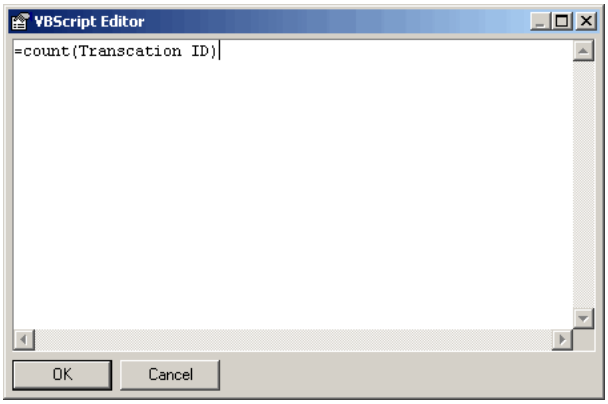
- Click **Label** , then drag the pointer to draw a box in the report at the place you want to add a label. Name the label, then specify its font, color, and other properties. You can click and drag the label to adjust its placement in the report.

To add data fields

- Click **Data field** ab|, then draw a box on the report. Change the properties of the data field by right-clicking it, and then clicking **Properties**.

To create a VBScript expression

1. Click **Calculated field** Σ... on the toolbar. The **VBScript Editor** appears.



2. Type the VBScript expression. For example, type:

   ```
   =count (Transaction ID)
   ```

3. Click **OK**.
4. Drag the pointer and place it under the respective field where you want the result to display.
5. Click the **Preview** icon on the toolbar to view the result.

To insert images

1. Click **Picture**. The **Open** dialog box appears.
2. Click an image, and then click **Open**.
3. Drag the cursor to draw a box where you want the image to appear.

To delete fields

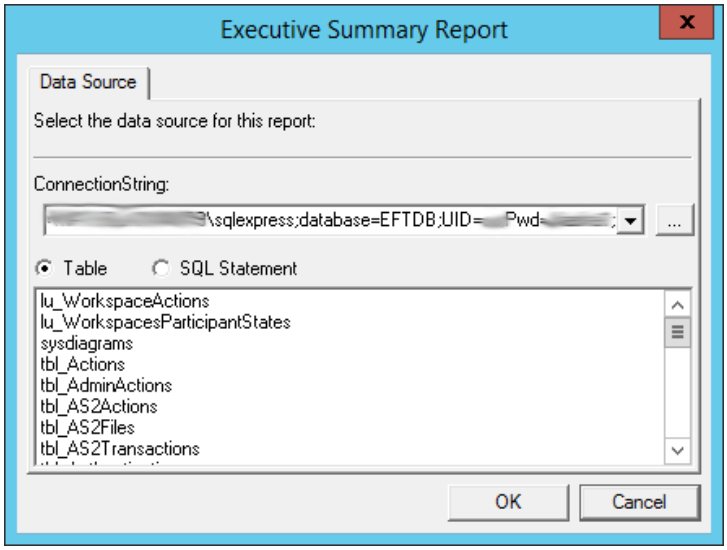
- Click the field, then press DELETE.

Changing the Data Source

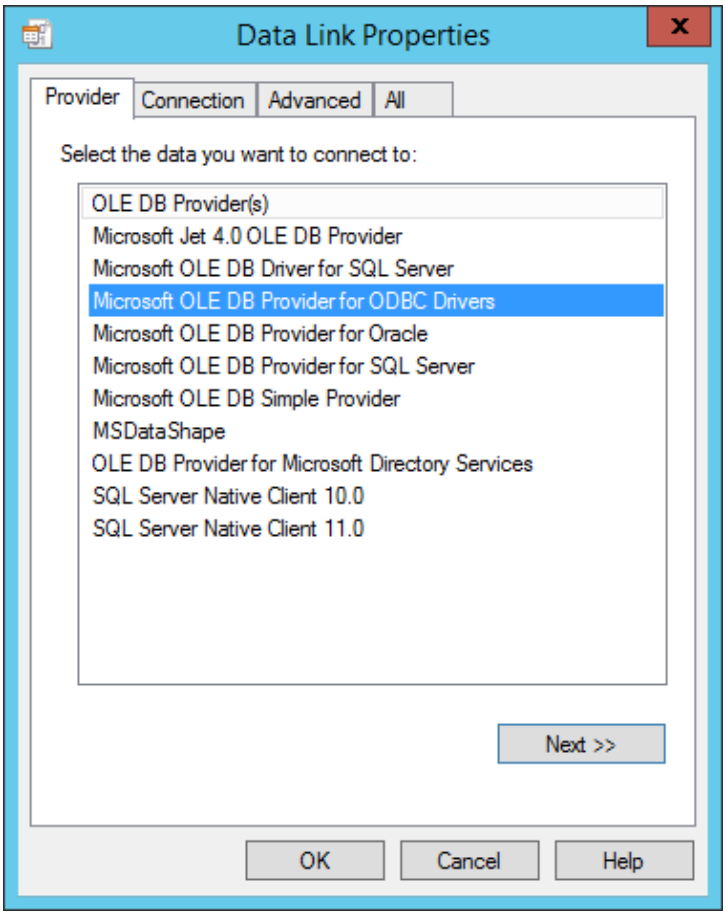
The data source is defined when you installed the ARM database. If you have more than one data source available, you can specify a different source.

To change the data source for a report

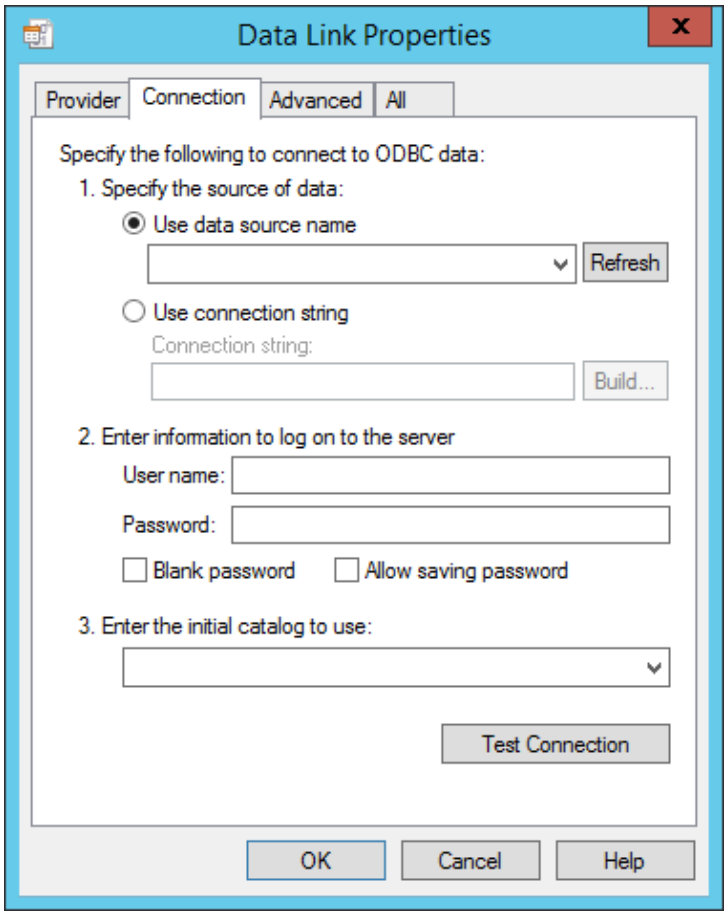
1. View the report in Design mode .
2. Click the **DataSource**icon. The wizard appears.



   - The title bar displays the name of the report.
   - The **ConnectionString**box is populated with the string that was defined when you installed ARM
   - The box below the ConnectionString displays the table or SQL Statement used to populate the report.
3. To specify a different data source, click the browse icon ... . The **Data Link Properties** dialog box appears.



4. In the **OLE DB Provider(s)**list, click the data source server (for example, **Microsoft OLE DB Provider for ODBC Drivers**), and then click **Next**. The **Connection** tab appears. What appears on the Connection tab depends on the OLE DB Provider selected.



5. In the **Select or enter a server name** box, click the down arrow, and then click the database host\instance name. If the server you want does not appear in the list, click **Refresh**. (If you still do not see the ARM database server, verify EFT's connection to the database on the Server's **Logs**tab.)
6. In the **Enter information to log on to the server** area, do one of the following:
    - Click use **Windows NT Integrated security**. The system will use the logged-in user's account for database connections.
    - Click **Use a specific user name and password**, then specify the username and password.
7. In the **Select the database on the server** box, click the down arrow and select the ARM database name.
8. Click **OK**. The wizard displays the data from the specified source.
9. Click **OK** to close the data source wizard.

    Refer to the System Requirements for the Microsoft OLE DB Driver version supported.

Grouping and Sorting Data

After designing the basic layout, you may decide to group the records by certain fields or other criteria to make the report easier to read. Grouping allows you to separate groups of records visually and display introductory and summary data for each group. The group break is based on a grouping expression. This expression is usually based on one or more recordset fields, but it can be as complex as you like.

Groups are also used for sorting the data, even if you do not plan to show the Group Header and Footer sections.

The bar across the top of each section (Page Header, Group Header, Detail) contains some useful tools and information about the section.

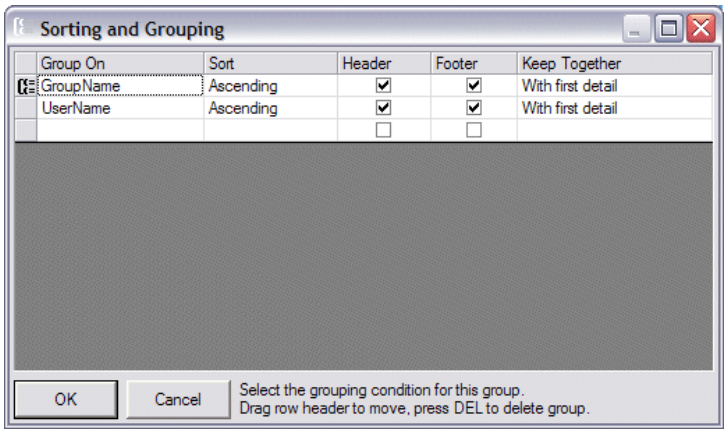
The indented box with a minus sign or a plus sign to the left of the section is used to collapse and expand the section. This feature is useful when you are designing the report to allow you to see a group's header and footer on the same screen without scrolling. Collapsing or expanding a section has no effect on how it is rendered in the report.

- An indented circle indicates that the section currently has zero height. You can drag the divider line down to increase the section's Height property.
- The triangle to the left of **Group Header** indicates the group's sorting order. You can click this icon to open the **Sorting and Grouping** dialog box.
- The labels to the right of the icons are the section name and, for group headers, the value of the group's **GroupBy** property (in this example, **Country**).

To add, edit, reorder, or delete groups in the report

1. Click the **Sorting and Grouping** icon, click **View >Grouping Window**, or click the triangle to the left of the group header. The **Sorting and Grouping** dialog box appears.

2. Use this dialog box to create, edit, reorder, and delete groups.



To create a new grouping condition

1. In the **Group On** column, click an empty row and type a name. For complex grouping, type an expression instead of a simple field name. For example, you could use "Country" to group by country or "Left(Country, 1)" to group by country initial.
2. In the **Sort** column, click the arrow to select the sort order you want to use for grouping the data (**Ascending**, **Descending**, or **None**).
3. In the **Header**, **Footer**, and **Keep Together** columns, specify whether the new group will have visible Header and Footer sections, and whether the group should be rendered together (**No**, **With first detail**, or **Whole Group**) on a page.

   You cannot use memo or binary (object) fields for grouping and sorting. This is a limitation imposed by OLEDB.

4. After you enter some data for the first group, a new blank row is appended to the list, so you can keep creating new groups. If you add more groups, you can change their order by clicking on the left-most gray cell in the row and dragging the row to a new position. This will automatically adjust the position of the Group Header and Footer sections in the report.
5. To delete a field in the group, select it, then press DELETE.
6. Click **OK**. The changes appear in the Designer.

Example: Creating a Custom Report

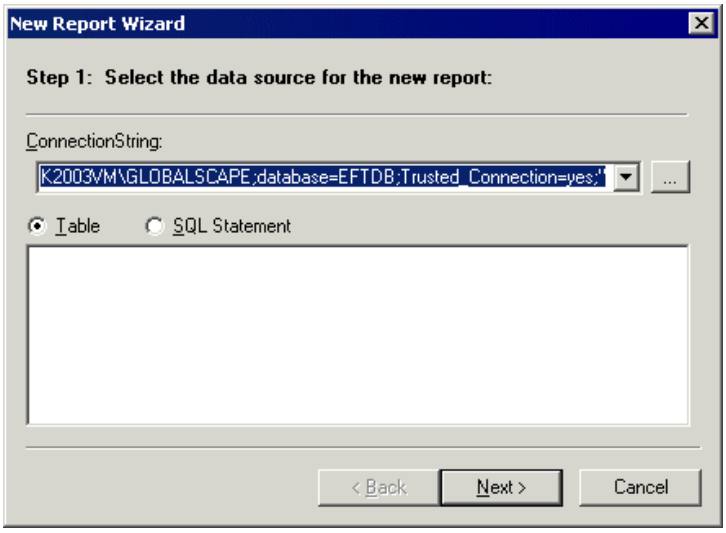
Below is an example of using the Report Wizard to create a custom administrator Actions report sorted by Site Name. The example assumes you have installed ARM with SQL Server Express and have performed administrator actions in EFT, such as creating users, stopping/starting sites, and so on.

To create the report

1. In the administration interface, connect to EFT, click the Site on which you want to create the report, then do one of the following:
   - On the toolbar, click the click **New Reports** icon .
   - On the main menu, click **Reports >New Report**.
   - Click the **Reports**tab, and then click the **New Report**icon New Report... on the bottom toolbar.

   The **Create New Report** dialog box appears.
2. Type a title for the new report, and then click **Create**. The **Report Designer** appears.

   So far, all you have done is opened the VSReport Designer, which allows you to open the **New Report Wizard**, which we will do next. You will delete this "template" later.
3. Click **File >New Report** or click the **New Report** icon on the VSReport Designer toolbar. The **New Report Wizard** appears.



4. By default, the **ConnectionString**box displays information for the database that you specified when you installed the Auditing and Reporting module (for example,

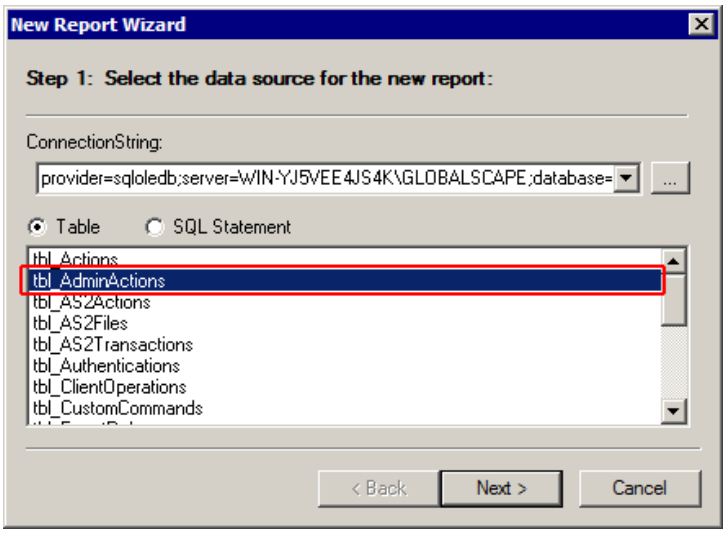
provider=SQLNCLI10;server=localhost\GLOBALSCAPE;database=EFTDB;Trusted_Connection=yes;). Click **Next** and go to step 5 or, if necessary, you can type a different string that is used to connect to the data source:

a. Click the ellipsis to define the connection string. The **Data Link Properties** dialog box appears.
b. On the **Provider**tab, click **Microsoft OLE DB Provider for SQL Server** as the provider to connect to the SQL Server database, and then click **Next**. The **Connection** tab appears.
c. In **Select or enter a server name**, click the arrow to select or type the name of EFT.
d. In **Enter information to log on to EFT**, click an authentication option to log on to EFT:
   - **Use Windows NT Integrated security** - Your computer automatically picks up the credentials from your computer and connects you to the database.
   - **Use a specific user name and password** - Specify the user name and the password to be used to log on to EFT. Select the **Allow saving password** check box to save the password in the connection string.

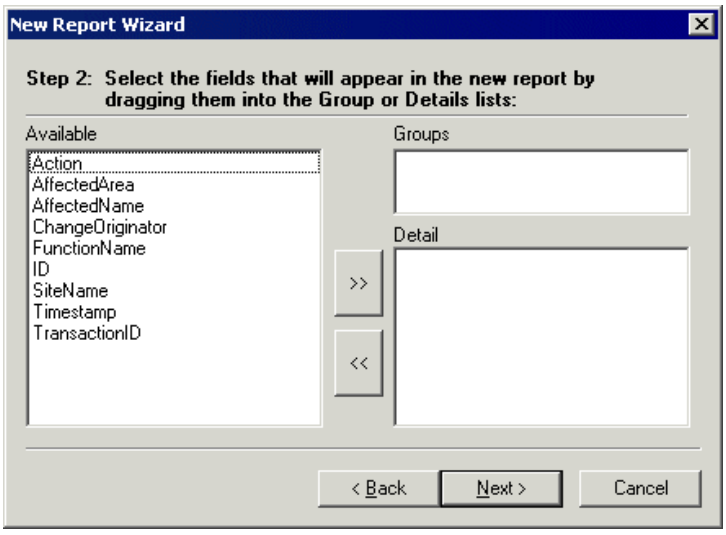
   > **NOTE:** Select the **Blank password** check box if EFT requires a blank password to log on the database server. Even if you do not type any password when you create a user account on a database server, you can select the **Allow saving password** check box. In this case, EFT takes a dummy password value and saves that value in the connection string. Selecting the **Blank password** check box disables the password field.

e. Click one of the following:
   - Select the database on EFT, and then click a database in the list.
   - Attach a database file as a database name - Click the ellipsis icon to browse for the SQL Server database file (*.mdf). The **Select SQL Server Database File** dialog box appears. Select a file, then click **Open**. The path to the file appears in the **Using the filename** box.
f. Click **OK**in the **Data Link Properties**dialog box to return to the **New Report Wizard**.

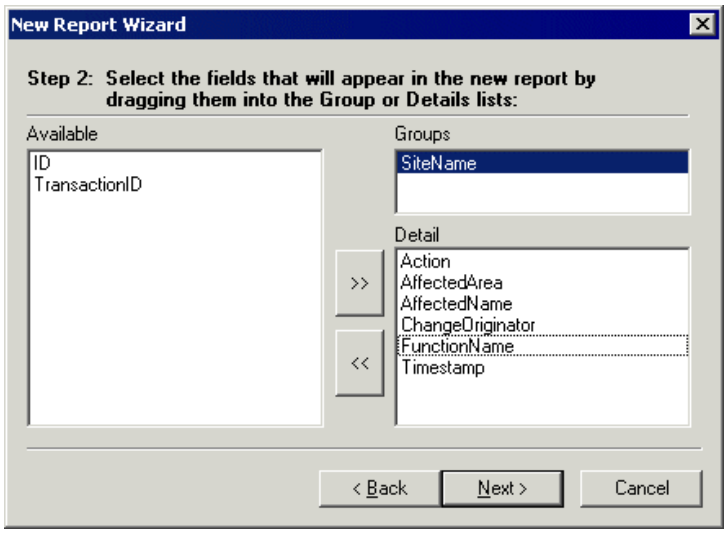
5. Click **Table**, then click **tbl_administratorActions**.



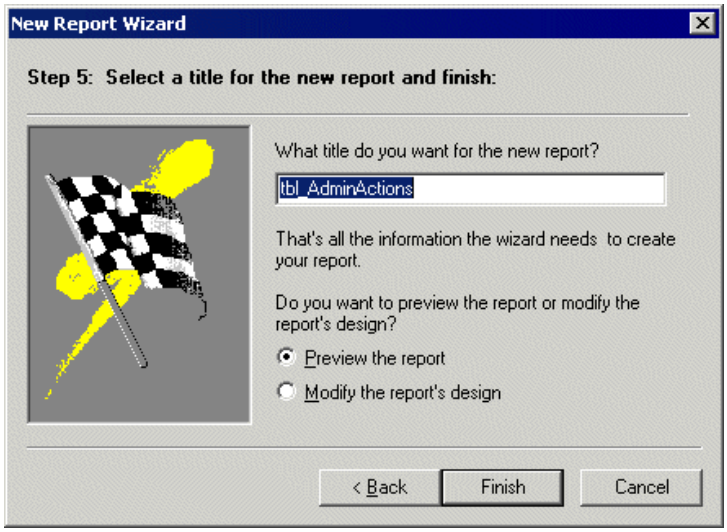
6. Click **Next**. The fields that appear in the **Available**list are from the table you selected in the previous step.



7. Click and drag **SiteName**to the **Groups** field, then click and drag each of the other fields, except **ID**and **TransactionID**, into the **Detail** box. (If you click the right-facing arrows, every field will move to the **Detail**area. Then you can individually move back the fields you do not want.)



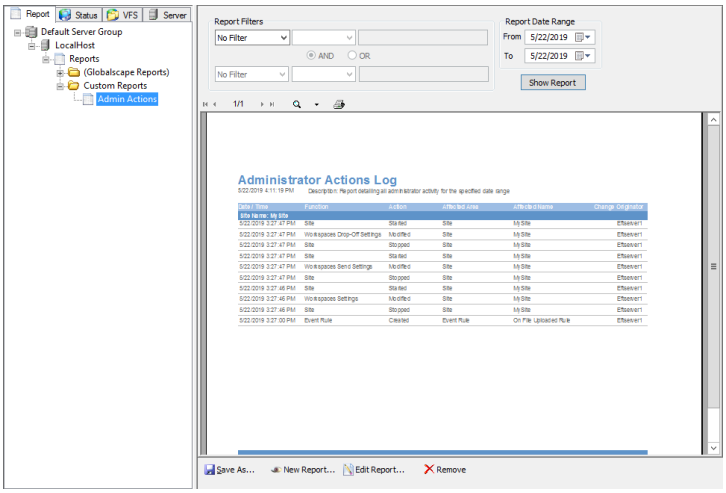
8. Click **Next**. The layout options appear.
9. Keep the default settings and click **Next**on each wizard page until you get to the last step. (For details of using the report wizard to define layout options, refer to Creating a Report with the Report Wizard. For this example, we used the default options.)



10. Type a title for the report, and then click **Finish**.
    - The left pane of the Report Designer displays the report's name (and the report template that was created in step 2).
    - The right pane displays a preview of the report.
    - The title bar displays the name of the report and an asterisk, indicating that you have not yet saved the report.
11. Let's get rid of that "new" template that was created when you opened the VSReport Designer. In the left pane, click the name of the template you want to remove, and then click the delete icon on the toolbar. Click **OK** to dismiss the

warning message.

12. Click **File > Save**or click the **Save** icon on the toolbar.
13. Click **File > Exit**to close VSReport Designer.
14. On the **Reports**tab, expand the **Custom Reports**node. The new report appears in the tree.
15. In the **Custom Reports**node, click to select the new report.
16. In the right pane, click **Show Report**. The report appears in the preview pane.



You can filter the results, such as show results only for certain Sites, a specific administrator account, or a certain date.

17. Click **Save As**to save the report. The report displays EFT administrator actions sorted by Site Name and Server.

Managing Reports

The topics below provide information regarding managing the reports of EFT activity.

- Saving a Report
- Exporting Reports in XML Format
- Exporting and Publishing Reports in the Report Designer
- Importing Reports
- Deleting a Report
- Saving Report Outputs
- Renaming a Report

Saving a Report

You can save reports to a file and export them in the following formats: HTML (.htm), VSPrinter (.vp), Portable Document Format (.pdf), Rich-Text Format (RTF), or plain text (.txt). (See Exporting and Publishing Reports in the Report Designer for a description of the various formats.)

To export a report

1. In the administration interface, connect to EFT and the reports database, and click the **Report** tab.
2. With the report displayed in the right pane, click **Save As**.
3. In the **Save as** dialog box, specify the format and location to save the report, then click **Save**.

Exporting Reports in XML Format

You can save (export) EFT reports in XML format, and they can be imported in that format.

To export the report

1. In the administration interface, connect to EFT and click the **Report** tab.
2. In the left pane, click the report.
3. On the main menu, click **Reports >Export Report** or right-click the report and click **Export Report**. The **Save As** dialog box appears.
4. Specify a name (if you want to save it with a different name), location to save the report, and the file type to save it as (XML), and then click **Save**.

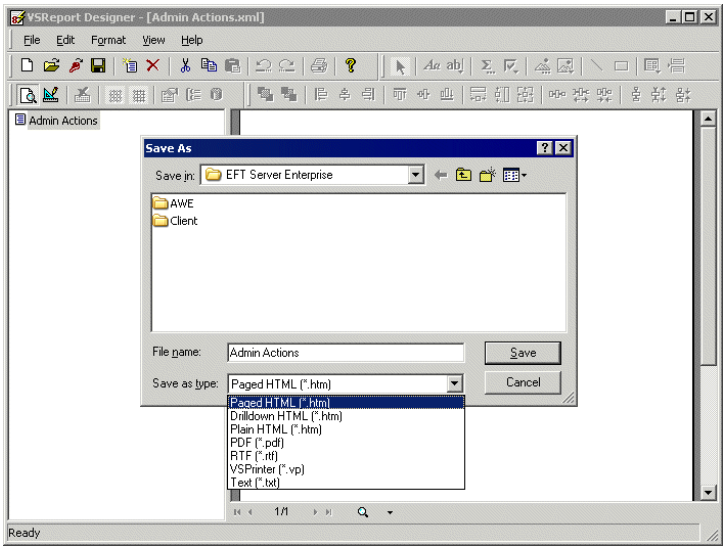
Exporting and Publishing Reports in the Report Designer

Instead of printing the report, you may want to export it into a file and distribute it electronically to your clients or coworkers. VSReport Designer supports several export formats, listed below:

Format	Description
Paged HTML	Creates one HTML file for each page in the report. The HTML pages contain links that let the user navigate the report.
Drill-Down HTML	Creates a single HTML file with sections that can be collapsed and expanded by the user by clicking on them.
Plain MILT	Creates a single, plain HTML file.
PDF	Creates a PDF file that can be viewed on any computer equipped with Adobe's Acrobat viewer or browser plug-ins.
VSPrinter	Creates a file using the VSPrinter control's native format. The file can be loaded, viewed, and printed from a VSPrinter control within an application or Web page.
Text	Creates a plain text file.

To create an export file

1. In the administration interface, connect to EFT and click the **Report** tab.
2. In the left pane, click the desired report.
3. In the right pane, click **Edit Report**. The report opens in the Report Designer.
4. In the left pane of the Report Designer, click the report that you want to export.
5. Click **File > Export**. The **Save As** dialog box appears.



6. Specify the type of file you want to create, its name (if you want to give it a different name), and its location, then click **Save**.

Importing Reports

You can add reports to EFT by importing the XML reports from the local drive to EFT.

To import reports into EFT

1. In the administration interface, connect to EFT and click the **Report** tab.
2. On the main menu, click **Report >Import** or right-click the **Reports** node and click **Import Report** from the shortcut menu. The **Open** dialog box appears.
3. Click the XML file you want to import, and then click **Open**.
4. The report is added in the left pane under **Reports**.

Deleting a Report

You can delete any reports that you no longer use. You cannot recover the report unless you previously exported and saved it.

To delete reports

1. In the administration interface, connect to EFT and click the **Report** tab.
2. In the left pane, click the report, then do one of the following:
   - On the main menu, click **Reports >Delete Report**.
   - Right-click the report and click **Delete Report**.
   - Click **Remove** .

   A confirmation message appears.
3. Click **Yes** to delete the report. The selected report is deleted and is not recoverable.

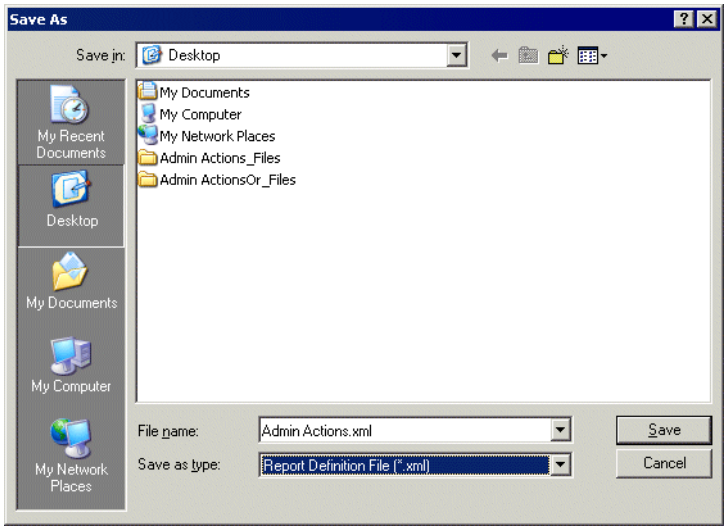
Saving Report Outputs

The report can be saved HTML, PDF, and XML.

To save reports in different formats

1. In the administration interface, connect to EFT and click the **Report** tab.
2. In the left pane, click the report, then do one of the following:
   - On the main menu, click **Reports >Save Report As**.
   - Right-click the report, and then click **Save Report Output As**.

   The **Save As** dialog box appears.



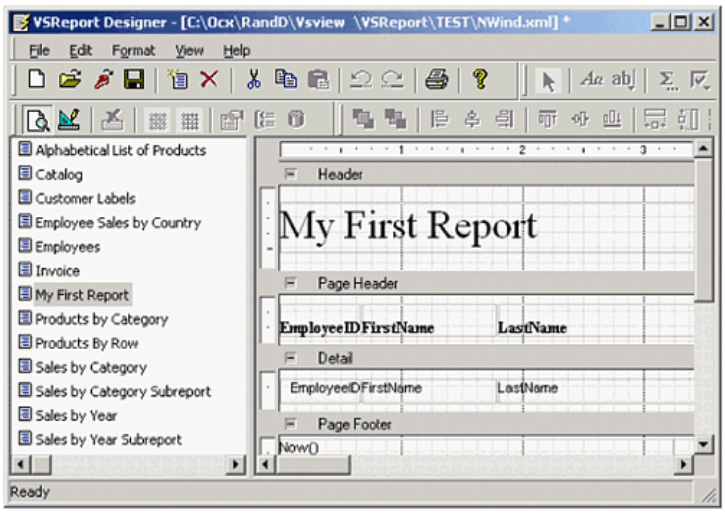
3. Navigate to the folder in which you want to save the report.
4. In the **File name** box, type a name for the report.
5. In the **Save as type** box, click a format, and then click **Save**.

Renaming a Report

You can rename the preconfigured reports and your custom reports, but you can't just type a new name in the tree. You have to open the Report Designer to rename the report.

To rename a report

1. In the administration interface, connect to EFT and click the **Reports** tab.
2. Click the report you want to rename, then click **Edit Report**. The report designer appears.



3. In the left pane of the report designer, click the report name to make it editable, type your changes, then press ENTER or click away from the edit box.
4. On the toolbar, click the **Save** icon, then close the Report Designer.

   The new name does not immediately update in the **Reports** tree of the administration interface. If you click or double-click the report in the tree, the name will update.

Regulatory Compliance Module

The topics below describe the Regulatory Compliance Module, used to accommodate user privacy, PCI DSS, and to meet GDPR requirements.

- Introduction to the Regulatory Compliance Module
- GDPR Settings
- GDPR Data Protection Officer
- GDPR-DPIA Report
- Personal Data Encryption
- Privacy Policy
- Terms of Service Agreement
- Specify GDPR Terms of Service and Privacy Policy Options
- PCI DSS Compliance

Introduction to the Regulatory Compliance Module

The Regulatory Compliance Module (RSM) helps you achieve or exceed compliance requirements mandated by the most rigorous standards, including PCI DSS, HIPAA, HITECH, Sarbanes-Oxley, and many others.

The features listed below are activated by the RCM:

- Privacy configuration, including GDPR-specific settings
- Specify personal data and privacy settings on a Site and per user (ARM Privacy reports require the Auditing and Reporting module.)
- Generate GDPR DPIA report (Requires ARM)
- Removes old data automatically Data sanitization/wiping (PCI DSS 9)
- Hides or disables non-allowed cipher or SSL versions, key lengths <128 bits, anonymous account type, and warns when importing certificates with weak keys (PCI DSS 4.1)
- Causes idle sessions to automatically timeout (PCI DSS 8.1.8)
- Limits repeated invalid login attempts (PCI DSS 8.1.6)
- Provides a configuration wizard for creating PCI DSS compliant Sites
- Monitors and reports on configuration changes that result in PCI DSS violations (PCI DSS 12) (Requires ARM)
- Produces automatic daily PCI DSS Compliance reports (PCI DSS 12) (Requires ARM)
- Warns if password complexity is disabled (PCI DSS 8.2.3)
- Warns if insecure protocols are in use (PCI DSS 2.2.2)
- Warns if user disk quota is not set (PCI DSS 3.1)
- Warns if secure remote administration not set (PCI DSS 2.3)
- Warns if Encrypting File System (EFS) in use (PCI DSS 3.4.1)
- Warns if weak SSL or SFTP keys are in use (PCI DSS 3.6.1)
- Warns if DoS and flood settings are too low (PCI DSS 2.2.4)
- Warns if vendor defaults remain unchanged (PCI DSS 2.1)
- Warns if expired keys present (PCI DSS 3.6.5)
- Warns if multiple administrator roles present (PCI DSS 7.1)
- Warns if anonymous account type in use (PCI DSS 8.5)

GDPR Settings

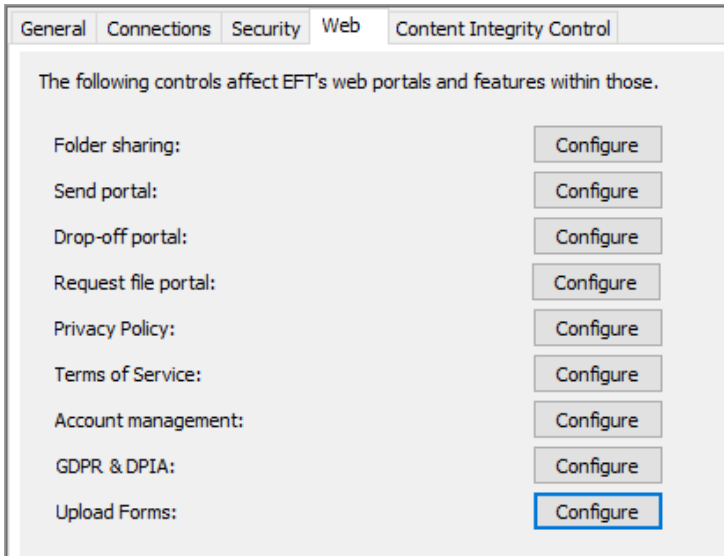
(Requires Regulatory Compliance Module) The General Data Protection Regulation (GDPR) is a part of European Union (EU) law regarding data protection and privacy in the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The GDPR applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of data subjects. The GDPR Settings in EFT can also be used to address other privacy regulations, such as California's CCPA and HIPAA.

EFT and the Web Transfer Client provide settings so that you can address each relevant article in the GDPR for those who access EFT and the Web Transfer Client. For example, the "Right to be Forgotten" (delete account) is part of the GDPR's data privacy rules. A user can exercise their right to be forgotten in their account profile, if the EFT administrator has configure Article 17 to be "Exercised via EFT's web client."

When the module expires,the **GDPR Settings** dialog box appears dimmed. However, you can still create Event Rules to an EU Data Subject's status, such as creating a **File Uploaded**event with a **User account** action set to change the user's status. Therefore, if your trial expires, examine your Event Rules and adjust as needed.

To configure the GDPR settings

1. In the administration interface, connect to EFT and in the left pan, click the **Site**.
2. In the right pane, click the **Web** tab.



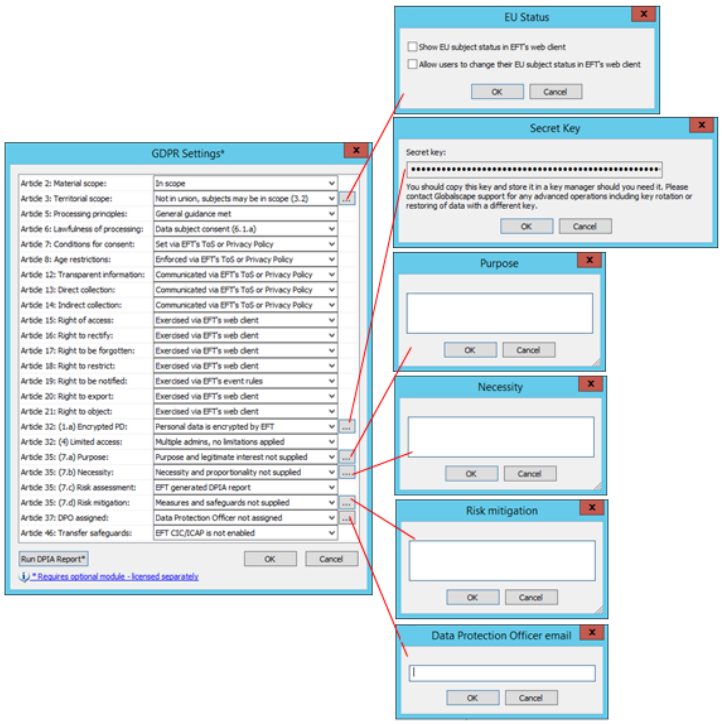
3. Next to GDPR & DPIA, click **Configure**. The **GDPR Settings** dialog box appears.

4. Refer to Article-by-Articlesettings below for guidance on how to configure each article.

The **GDPR Settings** dialog box is used to specify an Article-by-Article setting for user privacy policy for EFT web portals that may be accessed or shared with EU members.

Each of the applicable articles is listed in the **GDPR Settings** dialog box with a drop-down list with which you specify the setting. For example, the setting could be **Not applicable** or **Doesn't apply**if no EU members are expected to have user accounts on EFT.

For the Purpose, Necessity, Risk mitigation, and DPO assigned articles, when you click its **Browse** button, another dialog box appears in which you can provide additional data, such as the email address of the Data Protection Officer. A data protection impact assessment (DPIA) report can be run from this dialog box after the articles are each defined. The logged in administrator account must have **Manage reporting** and **Manage personal data permission**set in the server's **administration**tab. (The server administrator account is assigned these permissions by default when the account is created.)



Certain GDPR articles (described below in Article-by-Article settings) must be set to "Exercised via EFT's web client" for the setting to appear in the user account's profile in the WTC.

Article-by-Article settings

Items in the list below that are marked with a single asterisk * are default settings. However, if Material scope is set to Not in scope, then all items below marked with a double asterisk ** become the defaults. The numbers indicate the level of risk with that setting. For example, "Not in scope" is 0 risk; Unknown or Undefined is 1 for that article. The higher the total number of all of the articles assessed, the more risk there is. With the default settings, the total risk number is 21.

- Article 2: Material scope: Specify whether the operations carried out by EFT, or users managed by EFT, fall within scope of GDPR regulations.
  - Unknown or undefined* 1
  - In scope 0
  - Not in scope (2.2) 0 (If you select this value, then all remaining controls appears dimmed/unselectable, and the defaults marked with ** are applied.)
- Article 3: Territorial scope: Specify whether the territorial scope. Note that if **In Union** is chosen, all accounts will be marked as EU Data Subjects by default.
  - Unknown or undefined* 1
  - In Union, all subjects in scope (3.1) 0 (If you select this value, then EFT automatically, optionally, modifies each "Unknown" to "Yes" for EU data subject status.)
  - Not in union, subjects may be in scope (3.2) 0
  - In scope due to international laws (3.3) 0
  - Territory doesn't apply (not in scope)** 0
  - Click the browse button to specify that EU subject status should appear in the Web Transfer Client, and whether the user can change their EU subject status in the WTC.
- **Article 5: Processing principles**: Specify whether your assessment, with oversight from your Data Protection Officer, indicates that in context of EFT's operations, Article 5 principles have been met
  - Unknown or undefined* 1
  - General guidance not yet met 1
  - General guidance met 0
  - Principles don't apply (not in scope)** 0

- **Article 6: Lawfulness of processing:** Specify what the legal basis is for processing of PD with regard to EFT's file transfer operations or user account details or fields that might contain PD.
  - Unknown or undefined* 1
  - Data subject consent (6.1.a) 0 (If you select this setting, then EFT checks for users that are EU data subject accounts where consent was rescinded or denied and contain personal data.)
  - Contractual, vital interest, et. al. (6.1.b-f) 0
  - Other basis (6.2-4) 0
  - No PD is processed or stored for user 0
  - Not applicable (N/A)** 0
- **Article 7: Conditions for consent:** Specify whether data subjects have been provided with a mechanism for both providing or rescinding consent, in context with personal data stored by EFT or transferred by EFT.
  - Unknown or undefined* 1
  - Set via EFT ToS or Privacy Policy agreement 0
  - Set via external ToS or Privacy Policy agreement 0
  - Other method that can be demonstrated 0
  - Not applicable (N/A)** 0
- **Article 8: Age restrictions:** Specify whether you have measures in place to adhere to the age-restriction rules specified under Article 8, with regard to minors, in the context of EFT operations.
  - Unknown or undefined* 1
  - Enforced via EFT ToS or Privacy Policy 0
  - Enforced via external ToS or Privacy Policy 0
  - Enforced via other means 0
  - Not applicable (N/A)** 0
- **Article 12: Transparent information:** Specify whether you have mechanisms in place to clearly communicate to EU data subjects how, when, where, and why personal data is collected, used, stored, etc.
  - Unknown or undefined* 1
  - Communicated via EFT's Privacy Policy 0
  - Communicated via external Privacy Policy 0
  - Communicated via other means 0
  - Not applicable (N/A)** 0

- **Article 13: Direct collection:** Specify how information is conveyed in compliance with Article 13 when personal data was obtained directly from the data subject (such as via account self-provisioning).
  - Unknown or undefined* 1
  - Communicated via EFT's Privacy Policy 0
  - Communicated via external Privacy Policy 0
  - Communicated via other means 0
  - Not applicable (N/A)** 0
- **Article 14: Indirect collection:** Specify how information is conveyed in compliance with Article 14 when personal data was obtained indirectly from the data subject (such as via Active Directory provisioning).
  - Unknown or undefined* 1
  - Communicated via EFT's Privacy Policy 0
  - Communicated via external Privacy Policy 0
  - Communicated via other means 0
  - Not applicable (N/A)** 0
- **Article 15: Right of access:** Specify the means by which users can access the personal data associated with their account or stored on their behalf or transferred by them, if applicable.
  - Unknown or undefined* 1
  - Exercised via EFT's web client 0
  - Exercised upon request 0
  - Exercised via other means 0
  - Not applicable (N/A)** 0
- **Article 16: Right to rectify:** Specify the means by which data subjects can modify (rectify) the personal data associated with their account or stored on their behalf or transferred by them, if applicable.
  - Unknown or undefined* 1
  - Exercised via EFT's web client 0
  - Exercised upon request 0
  - Exercised via other means 0
  - Not applicable (N/A)** 0

- **Article 17: Right to be forgotten:** Specify the means by which data subjects can request deletion of their account and removal of their personal data, were applicable, in context with EFT.
  - Unknown or undefined* 1
  - Exercised via EFT's web client 0
  - Exercised upon request 0
  - Exercised via other means 0
  - Not applicable (N/A)** 0
- **Article 18: Right to restrict:** Specify the means by which data subjects can restrict access to or use of the personal data associated with their account or stored on their behalf or transferred through EFT.
  - Unknown or undefined* 1
  - Exercised via EFT's web client 0
  - Exercised upon request 0
  - Exercised via other means 0
  - Not applicable (N/A)** 0
- **Article 19: Right to be notified:** Specify the means by which data subjects are notified if their personal data is modified or deleted, within EFT context, if applicable.
  - Unknown or undefined* 1
  - Exercised via EFT's event rules 0
  - Exercised upon request 0
  - Exercised via other means 0
  - Not applicable (N/A)** 0
- **Article 20: Right to export:** Specify the means by which EU data subjects can export a copy of the personal data associated with their account or stored on their behalf or transferred by them, if applicable.
  - Unknown or undefined* 1
  - Exercised via EFT's event rules
  - Exercised via EFT's web client 0
  - Exercised upon request 0
  - Exercised via other means 0
  - Not applicable (N/A)** 0

- **Article 21: Right to object:** Specify the means by which users can object to the use of the personal data associated with their account or stored on their behalf or transferred by them, if applicable.
  - Unknown or undefined* 1
  - Exercised via EFT's web client 0
  - Exercised upon request 0
  - Exercised via other means 0
  - Not applicable (N/A)** 0
- **Article 32: (1.a) Encrypted PD:** EFT selects the default based on current configuration, whether user account fields marked as personal data are encrypted. You can select a value, if desired.
  - EFT is not encrypting PD* 1
  - EFT is encrypting PD* 0
  - A compensating control is in place 0
  - Not applicable (N/A)** 0
- **Article 32: (4) Limited access:** EFT selects the default based on whether there is more than one EFT administrator, and if so, whether at least one does NOT have access to personal data.
  - Multiple administrators, no limitations applied* 1
  - Multiple administrators, limitations applied* 0 (EFT automatically sets the default depending on configuration; if set, the other items are not available for selection.)
  - Single administrator, requires full access* 0
  - A compensating control is in place 0
  - Not applicable (N/A)**

- **Article 35: (7.a) Purpose:** This article requires that you document the express purpose and legitimate interest for processing of personal data, for the DPIA report.
  - Purpose and legitimate interest supplied 0, not supplied* 1 (A **Browse** button opens a dialog box in which you can supply the purpose and legitimate interest. If data is in provided in the dialog box, then "supplied" is displayed; however, you can still select N/A if desired.)
  - Other or external measures 0
  - Not applicable (N/A)** 0
- **Article 35: (7.b) Necessity:** This article requires that you document the necessity and proportionality of the processing operations in relation to the purposes, for the DPIA report.
  - Necessity and proportionality supplied 0, not supplied* 1 (A **Browse** button opens a dialog box in which you can note the necessity. If data is in provided in the dialog box, then "supplied" is displayed; however, you can still select N/A if desired.)
  - Other or external measures
  - Not applicable (N/A)** 0
- **Article 35: (7.c) Risk assessment:** This article requires that you document the risks to the rights and freedoms of data subjects. EFT's DPIA report can assist with fulfilling this requirement.
  - EFT generated DPIA report* 0
  - Other or external measures 0
  - Not applicable (N/A)** 0
- **Article 35: (7.d) Risk mitigation:** This article requires that you document the measures and safeguards to mitigate risks to the rights and freedoms of data subjects.
  - Measures and safeguards supplied 0, not supplied* 1 (A **Browse** button opens a dialog box in which you can note the risk mitigation. If data is in provided in the dialog box, then "supplied" is displayed; however, you can still select N/A if desired.)
  - Other or external measures
  - Not applicable (N/A)** 0
- **Article 37: DPO assigned:** Specify the email address for the Data Protection Officer (DPO) or equivalent. (The email variable %SERVER.PRIVACY_DPO_EMAIL% can be used in Event Rules.)

- Data Protection Officer assigned 0, not assigned* 1 (A **Browse** button opens a dialog box in which you can provide the email address of the DPO.)
- Other or external measures 0
- Not applicable (N/A)** 0

- **Article 46: Transfer safeguards:** Specify whether EFT is configured to use its Content Integrity Control (CIC) action or external process for identifying personal data contained within transferred files
    - EFT CIC/ICAP is enabled 0, not enabled* 1 (Similar to Article 32 (encryption), EFT will auto detect if ICAP is enabled and preselect the correct value accordingly. You can still change to external or N/A if desired.)
    - Other or external measures 0 (If ICAP is enabled, EFT checks if there are any affected rules that either process files, such as Folder Monitor, File Uploaded, Folder Downloaded, or have Copy/Move operations defined that are missing the CIC action.)
    - Not applicable (N/A)** 0

Related Topics

- GDPR Data Protection Officer
- Privacy Policy
- Terms of Service Agreement
- Specify Terms of Service and Privacy Policy Options
- WTC & Workspaces Administration

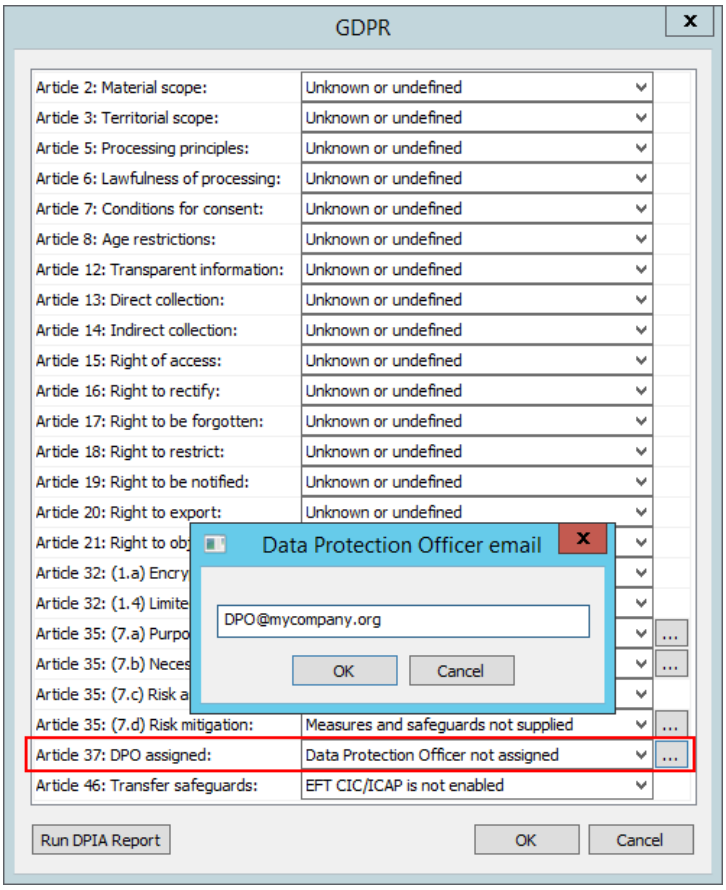
GDPR Data Protection Officer

Article 37 of the GDPR requires the designation of a Data Protection Officer (DPO) when you require regular and systematic monitoring of EU data subjects. Because EFT requires user account information, there are certain GDPR articlesthat you must adhere to, as shown in the GDPR dialog box below. The DPO is especially necessary when processing special categories of personal data, such as race, religion, genetic or biometric data, or even trade union membership (Article 9), or personal data relating to criminal convictions and offences (Article 10).

To provide the DPO email address

1. On the **Site > Web**tab, next to GDPR and DPIA, click **Configure**.
2. Next to **Article 37**, click the drop-down list to add an email address for the DPO. If a DPO is not necessary, you can choose one of the following: **Data Protection Officer not assigned**, **Not applicable (N/A)**, or you are deploying **Other or external measures**.
3. If you chose **Data Protection Officer not assigned**, click the browse button to open the **Data Protection Officer email** dialog box.
4. Type an email in the box, then click **OK**.

   The list box changes to **Data Protection Officer is assigned**.



5. Click **OK** to close the **GDPR** dialog box.
6. Click **Apply** on the **Web** tab.

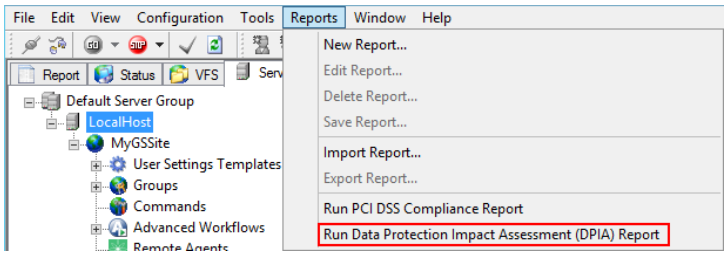
Related Topics

- GDPR Settings
- Privacy Policy
- Terms of Service Agreement
- Specify Terms of Service and Privacy Policy Options
- GDPR-DPIA Report
- Personal Data Encryption

GDPR-DPIA Report

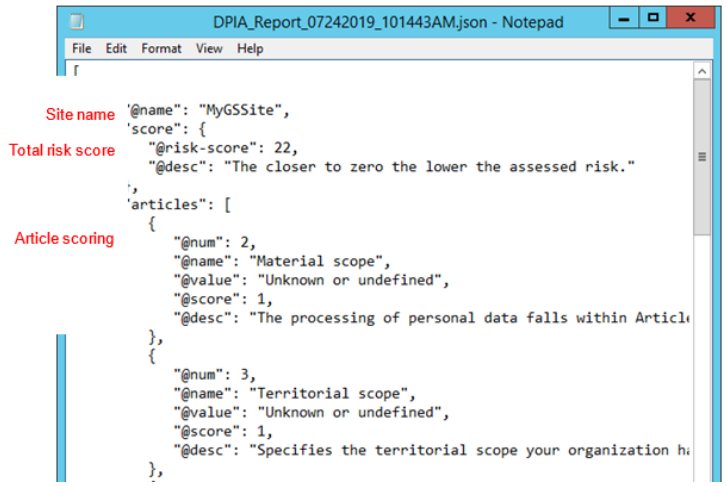
The GDPR Data protection impact assessment (DPIA) helps you identify and minimize the risks to your data. On the Site's Webtab, when you configure the GDPR settings, you can generate the DPIA report, and a JSON file is created and saved in the EFT installation directory, in the **/Generated Reports/** folder. (The default is **C:\ProgramData\Globalscape\EFT Server\GeneratedReports**.) The date and time are appended to the file name, as shown in the screen shot below. The contents of the file are taken from the configuration you have set in the GDPR dialog box.

You can also run the report from the administration interface main menu:



Click the screenshot below to open the JSON file showing the default settings.

The DPIA report lists the Site name, total risk score, and individual scoring for each article. (Refer to GDPR Settings for more information about the articles.)



Related Topics

- GDPR Settings
- GDPR Data Protection Officer

- User Account Details Template
- Creating a User Account

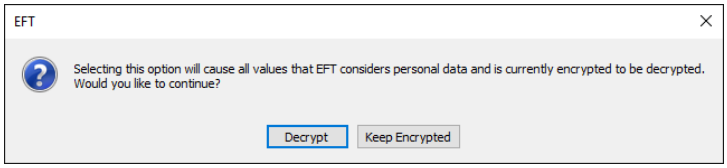
Personal Data Encryption

As the EFT administrator, you can enable or disable Personal Data encryption for all users. Users do not have the option individually to encrypt or not encrypt their data. The encryption property applies to all users on EFT.

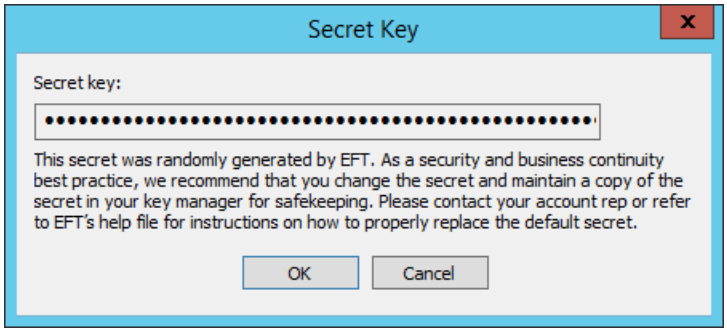
- EFT generates the Personal Data key upon new Site creation.
- Upon upgrade, EFT generates a new key if the Personal Data key is the old "default" value and personal data is not encrypted.
- If your organization has a policy of key rotation every "n" days, you can replace the Personal Data Key manually.

To change the personal data encryption key

1. In the **GDPR Settings**dialog box, scroll to **Article 32: (1.a.) Encrypt PD**.
2. Disable encryption of personal data by selecting **Personal Data is not encrypted by EFT**, then click **Decrypt**. After EFT finishes decrypting, you can supply a new Personal Data encryption key.



3. Select **Personal data is encrypted by EFT**, then click the browse icon to provide a new secret key. The key must be exactly equal to 64 hexadecimal characters.



4. Click **OK** to save the key, then click **OK** to close the **GDPR Settings** dialog box.
5. Click **Apply** to save your changes.

Related Topics

- Advanced Properties
- GDPR Settings
- Specify GDPR Terms of Service and Privacy Policy Options
- User Account Details Template

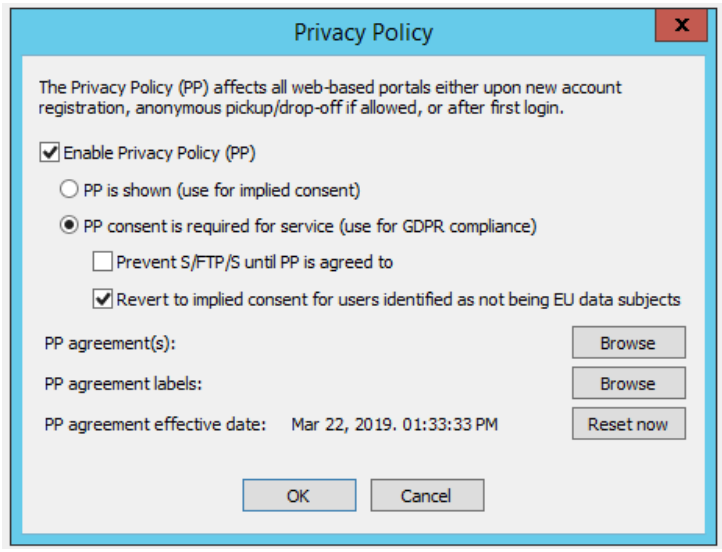
Privacy Policy

(Requires HTTP/S, Workspaces, RCM) You can create and display a Privacy Policy for all web-based access to EFT. The Privacy Policy affects all web-based portals upon new account registration, anonymous pickup or drop-off, and upon first login. For user-specific settings, refer to Specify Terms of Service and Privacy Policy Options.

- If accessing EFT for the first time via FTP, FTPS, or SFTP, and the Privacy Policy consent is required for use, the connection will fail. The user must first connect via the Web Transfer Client (HTTPS portal) to consent to the policy. The administrator can instead set the status for the Privacy Policy for a given user manually, on user account's **General**tab in the EFT administration interface. Additionally, you can change the EFT login banner to provide instructions to login via the Web Transfer Client before logging in via FTP, FTP, or SFTP.
- If the Privacy Policy is set to the default (enabled, but not mandatory) and the user implicitly agrees to the policy by continuing to use the service, then no record is audited to the EFT database.
- For anonymous users, accepting the Privacy Policy sets a cookie for 12 hours so that the user doesn't have to consent for each action within that 12 hours.
- For an example of a Privacy Policy, refer to https://policies.google.com/privacy.

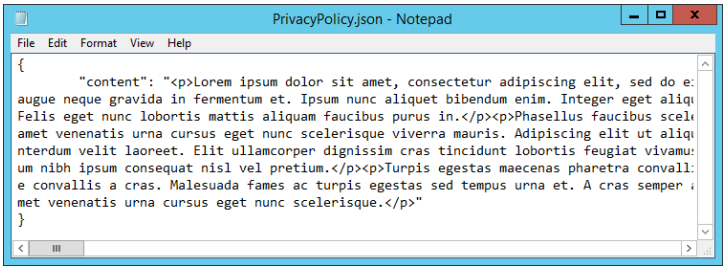
To enable the Privacy Policy agreement

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. On the **Web**tab, next to **Privacy Policy**, click **Configure**. The **Privacy Policy** dialog box appears.



4. Select the **Enable Privacy Policy** check box, then specify whether the agreement is **implied** or **required for service**. If the agreement is required, you can select the **Prevent** check box to prevent access over FTP, SFTP, or FTPS until the Privacy Policy agreement is accepted. The **Revert to implied consent for users identified as not being EU data subjects**is selected automatically.
5. To select or view the agreement(s) or the agreement labels, click **Browse**. Windows Explorer opens to the **\Web**folder.
6. The **\Templates**folder contains the **PrivacyPolicy.json**file. Replace the default text with your organization's Privacy Policy.

   The **PrivacyPolicy.json** file contains "dummy text" ("lorem ipsum dolor...") that you will replace with the text of your policy.



You can use basic HTML formatting tags (<p>, <li>, etc.). The "content" label must be kept, as well as opening and closing curly brackets { } :

```
{
 "content": "<p>This is our Privacy Policy ... </p>"
}
```

7. Refer to **Edit the Privacy Policy and labels** for how to edit the Privacy Policy and agreement labels files.
8. To reset the agreement effective date, such as when publishing a new agreement, click **Reset now**.
9. Click **OK**, then click **Apply** on the **Web** tab. A Site restart is required.

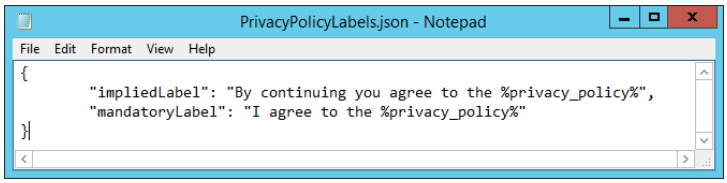
Edit the Privacy Policy and Labels

The **PrivacyPolicy** and **PrivacyPolicyLabels** files are JSON files (similar to XML) that must be edited for your organization's agreement. (The labels in the JSON file are case-sensitive.) The files are saved in:

C:\Program Files\Globalscape\EFT Server\Web\Templates

1. Open the **PrivacyPolicyLabels.json**file and the **PrivacyPolicy**.json file in a text editor, such as Notepad.
2. Save a copy of each before you edit the originals so you have a backup.

   The **PrivacyPolicyLabels** file is used to change the default text that appears when you have specified that the Privacy Policy is implied or when it's mandatory to continue. For example, the default text when the agreement to the policy is mandatory is, in English, "I agree to the Privacy Policy."



3. Change the value (By continuing...") to whatever your organization requires, or to another language. However, do not change any the label variables (impliedLabel, mandatoryLabel) or the text that is between the % signs. The opening and closing curly brackets { } are also required.

Related Topics

- Logging In (accepting Privacy Policy)
- Specify GDPR status, Terms of Service, and Privacy Policy Options
- GDPR Data Protection Officer
- GDPR Settings
- Terms of Service Agreement
- Specify Terms of Service and Privacy Policy Options

GDPR Right Exercised

The **GDPR Right Exercised** event is triggered based on the **If Event Reason**Condition specified. You can specify that the Event Reason "does" or "does not" equal one of the following behaviors:

- The user has rescinded consent
- The user has accessed (viewed) their personal data
- The user has had rectified (modified) their personal data
- The user has asked to be forgotten
- The user has asked to restrict the use of their personal data
- The user has asked to restrict the use of their personal data
- The user's personal data has been modified by someone other than the user
- The user has ported (exported) their personal data
- The user has objected to the use of their personal data

For example, you could define an Event Rule to send an email notification when a user's personal data is modified by someone other than the user, such as an administrator.

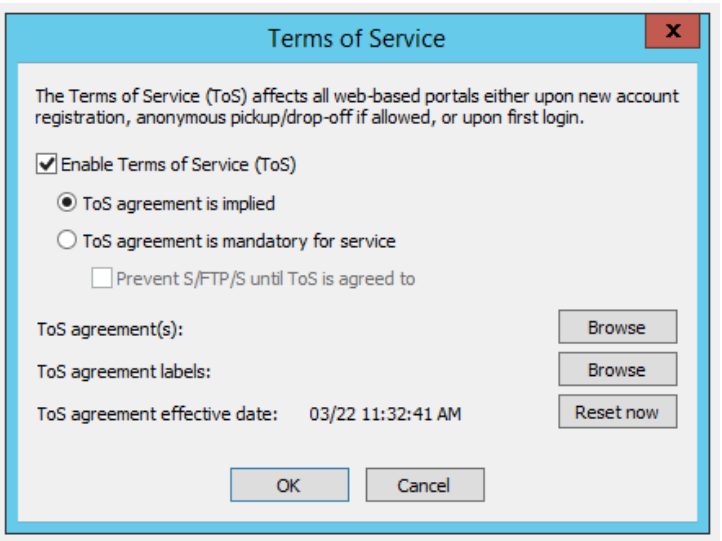
Terms of Service Agreement

(Requires HTTP/S, Workspaces, RCM) The EFT web portal Terms of Service agreement can be used to identify or specify whether a user has consented to use of their personal data. This information can help you stay in compliance with GDPR and other privacy regulations. From the Site's **Web**tab, you can configure the Terms of Service agreement, which affects all users on the Site, all web-based portals upon new account registration, anonymous pickup or drop-off, and upon first login. For user-specific settings, refer to Specify Terms of Service and Privacy Policy Options.

- If accessing EFT for the first time via FTP, FTPS, or SFTP, and the Terms of Service agreement is mandatory for service, the connection will fail. The user must first connect via the Web Transfer Client (HTTPS portal) to accept the Terms of Service. The administrator can instead set the status for the Terms of Service for a given user manually, on user account's **General**tab in the EFT administration interface. Additionally, you can change the EFT login banner to provide instructions to login via the Web Transfer Client before logging in via FTP, FTP, or SFTP.
- If the Terms of Service agreement is set to the default (enabled, but not mandatory) and the user implicitly agrees to the Terms of Service (by continuing to use the service), then no record is audited to the EFT database.
- For anonymous users, accepting the Terms of Service sets a cookie for 12 hours so that the user doesn't have to consent for each action within that 12 hours.
- For an example of a Terms of Service agreement, refer to https://policies.google.com/terms.

To enable the Terms of Service agreement

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. On the **Web**tab, next to **Terms of Service**, click **Configure**. The **Terms of Service** dialog box appears.



4. Select the **Enable Terms of Service** check box, then specify whether the agreement is **implied** or **mandatory for service**. If the agreement is mandatory, select the **Prevent** check box to prevent access over FTP, SFTP, or FTPS until the Terms of Service agreement is accepted.
5. To view the agreement(s) or the agreement labels, click **Browse**. The Windows File Explorer opens to the EFT installation folder. You can't actually "browse for files." Instead, you must edit the JSON file, as described in the next section.)
    - Refer to Edit the Terms of Service agreement and agreement labels for how to edit the Terms of Service agreement and agreement labels files.
6. To reset the agreement effective date, such as when publishing a new agreement, click **Reset now**.
7. Click **OK**, then click **Apply** on the **Web** tab.

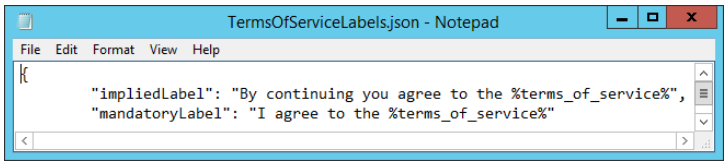
Edit the Terms of Service Agreement and Agreement Labels

The **TermsOfService** agreement and **TermsOfServiceLabels** files are JSON files (similar to XML) that must be edited for your organization's agreement. (The labels in the JSON file are case-sensitive.)

1. Save a copy of each before you edit the originals so that you have a backup.
2. Open the **TermsOfServiceLabels.json**file and the **TermsOfService.json**file in the EFT installation folder, in a text editor, such as Notepad.

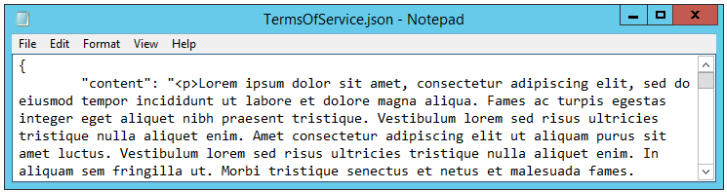
    C:\Program Files\Globalscape\EFT Server\Web\Templates

The **Labels** file is used to change the default text that appears when you have specified that the Terms of Service are implied or when it's mandatory to continue. For example, the default text when the agreement to the terms is mandatory is in English, "I agree to the terms of service."



3. Change the text to whatever your organization requires, or to another language. However, do not change any text that is between the quotation marks, as that is a variable used by EFT. The opening and closing curly brackets { } are also required.

   The **TermsOfService.json**file contains "dummy text" ("lorem inpsum dolor...") that you will replace with the text of your agreement:



4. Use basic HTML formatting tags (<p>, <li>, etc.) to create your Terms of Service. The "content" label must be kept, as well as opening and closing curly brackets { }.

```
{
 "content": "<p>These are the Terms of Service ... </p>"
}
```

5. You can make different Site-specific policies:
   a. Create a "Custom" folder under the **Web** directory and copy the **Templates** folder to the **Custom** folder that you just created: **…\Globalscape\EFT Server\Web\Custom\Templates**
   b. For server-specific customizations place the custom file in: **…\Globalscape\EFT Server\Web\Custom\Templates**
   c. For site-specific customizations place the custom file in: **…\Globalscape\EFT Server\Web\Custom\MySite\Templates** (With "Mysite" being the name of the Site it applies to.)

      You will need to clear the cache of the web browser to see your changes.

Related Topics

- Logging In (accepting Terms of Service)
- Specify GDPR status, Terms of Service, and Privacy Policy Options
- GDPR Data Protection Officer
- Privacy Policy
- GDPR Settings
- Specify Terms of Service and Privacy Policy Options

Specify GDPR Status, Privacy Policy Options, and Terms of Service for Users

The EFT Privacy Policy and web portal Terms of Service agreement can be used to identify or specify whether a user has consented to use of their personal data. This information can help you stay in compliance with GDPR and other privacy regulations. From the Site's **Web**tab, you can configure the agreements, which affect all users on the Site, all web-based portals upon new account registration, anonymous pickup or drop-off, and upon first login. For Site-specific settings, refer to Terms of Service Agreement, Privacy Policy, and GDPR settings.

If consent to use or store personal data is required for use of the service, then you should document WHY the user's consent is required. GDPR Article 7.4 mandates that "utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

Globalscape does not provide the text for your Privacy Policy or Terms of Service agreement. It is up to your organization to create that.

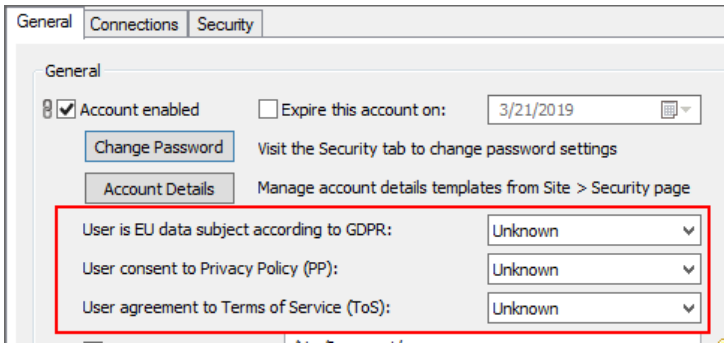
If the Privacy Policy or Terms of Service options are disabled on the **Web**tab, these options are still available on the user account's **General** tab, because the administrator can change them based on agreement or consent from the user, instead of in the browser.

The agreements can be "implicit" or "explicit" agreement:

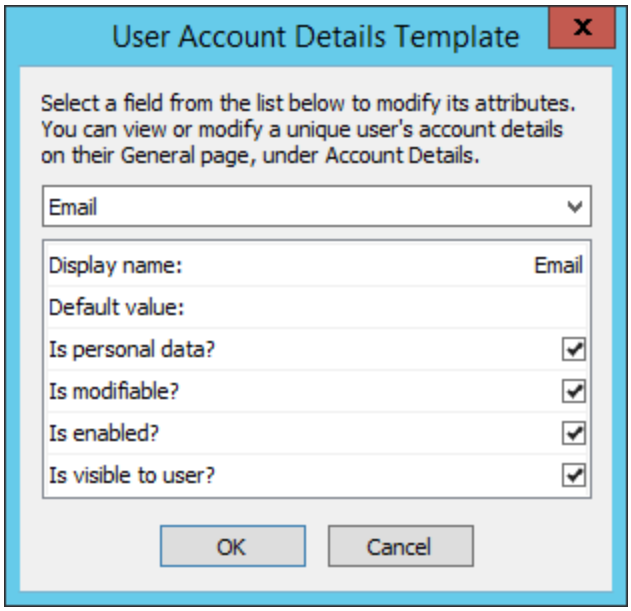
- **implicit** means agreement is implied or understood, e.g., when the user creates an account and provides personal data that is optional for use of the service. (To use EFT, the only required data is an email address and a username/password.)
- **explicit** means agreement is clearly stated, such as in a written agreement that the user account owner has accepted

To specify the user account's options

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the **user account** that you want to configure.
3. In the right pane, click the **General**tab.



4. Under **Account Details**, the **GDPR**, **Privacy**, and **Terms of Service** options appear.
    - **User is EU data subject according to GDPR** - Click **Unknown**, **Yes**, or **No**.
    - For **User consent to Privacy Policy**- Click **Unknown**, **Granted (implicit)**, **Granted (explicit)**, **Denied**, or **Rescinded**.
    - For **User agreement to Terms of Service** - Click **Unknown**, **Agreed (implicit)**, **Agreed (explicit)**, or **Disagreed**, or**Withdrawn**.
5. Click **Account Details**to provide name, company, email, and so on.
6. Go to the **Site**> **Security** tab to specify policies for each field in the **User Account Details Template.**



7. By default, each of the fields have the same policies: **Is personal data**, **Is modifiable**, **Is enabled**, and **Is visible to user**. If you want to change any of those options for any field, select the field in the drop-down, and then clear or select the applicable check box. The attributes in the template apply to all users in all Settings Templates on the Site.

8. Refer to Terms of Service Agreement and Privacy Policy for more configuration, including specifying the actual agreements.

Related Topics

- Logging In (accepting Privacy Policy and Terms of Service)
- Terms of Service Agreement
- User Account Details Template
- Privacy Policy
- GDPR Settings
- GDPR Data Protection Officer
- GDPR-DPIA Report
- GDPR Right Exercised User Events

PCI DSS Compliance

EFT can help you get and stay in compliance with the PCI DSS. (Requires RCM.) The topic below describe how PCI DSS compliance is addressed in EFT.

- PCI Data Security Standard
- How PCI DSS Requirements Addressed
- Possible Compliance Report Outcomes
- Warnings for PCI DSS Violations

Payment Card Industry (PCI) Data Security Standard (DSS)

In 1999, Visa USA developed the Cardholder Information Security Program (CISP). The goal of this program was to assure cardholders that their account information was safe, regardless of where it was offered for payment. Originally intended to secure credit card transactions over the Internet, the CISP was expanded and mandated in June 2001 to apply to all payment channels, including retail (brick and mortar), mail/telephone order, and e-commerce. To achieve CISP compliance, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI DSS, the result of collaboration between Visa and MasterCard, is designed to create common industry security requirements that incorporate the CISP requirements. Visa, MasterCard, American Express, Diner's Club, Discover, and JCB USA have each endorsed the CISP and PCI DSS. If a member, merchant, or service provider does not comply with the security requirements or fails to rectify a security issue, they could face fines of up to US$500,000 per incident, or restrictions imposed by the credit card companies, including denying the member's, merchant's, or service provider's ability to accept or process credit card transactions.

Who Must Comply with PCI?

Any organization that stores, processes, or transmits Primary Account Number (PAN) data must comply with PCI DSS requirements. However, even organizations that do not store or transmit PAN data may decide to use the PCI DSS requirement document as an internal security best practice guideline by which they measure and implement their own data security standards.

Refer to PCI DSS Requirements for information about specific PCI DSS requirements addressed in EFT.

- For more information regarding PCI Security Standards, including downloading a PDF of the standard, visit https://www.pcisecuritystandards.org/index.htm.
- For a list of terms and acronyms used in the standard, refer to https://www.pcisecuritystandards.org/tech/glossary.htm.

How EFT Addresses PCI DSS Requirements

EFT facilitates enforcing high security and compliance with the PCI Data Security Standard (PCI DSS), which provides detailed security compliance guidelines that can be used to provide hardened security for EFT, no matter which rules or standards by which your organization is measured. Each requirement and a description of how EFT helps comply with the requirements is described below.

Refer to the PCI Security Standards website for official documentation of the standard.

Compensating Controls

From the PCI DSS Security Auditing Procedures document:

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

When EFT warns you of a non-compliant setting, you will be given the choice to fix the problem or proceed with the non-compliant setting. If you choose to proceed in violation of the PCI DSS, you will be asked to specify a compensating control, i.e. an alternate hardware, software, or internal policy that satisfies the requirement in some other way (ref. "Compensating Controls" in the PCI DSS for more information). The controls you document will appear in the PCI DSS Compliance report, which you can provide to Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs), individuals who are certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS.

PCI DSS Requirements Addressed

EFT facilitates compliance with applicable PCI DSS requirements. The PCI DSS requirements related to physical security and cardholder database security are not applicable to EFT; however, you should place the Server computer in a secured area, such as a locked server room or network operations center.

Requirement 1: Install and Maintain Network Security Controls

- Storing cardholder in the DMZ or other untrusted network is expressly prohibited by PCI DSS. And for security best practices you should not allow inbound connections to originate from untrusted into trusted zones.
- EFT provides a robust set of IP access filters to control access to EFT and/or the DMZ Gateway.

- When EFT is used in combination with the DMZ Gateway, no internal inbound ports need be opened into the trusted network, hence all inbound traffic will be restricted to IP addresses within the DMZ.
- Your internal IP addressing scheme is never exposed when EFT is used in combination with the DMZ Gateway.

Requirement 2: Apply Secure Configurations to All System Components

- When you create a "strict security" site, EFT monitors and warns:
  - Whether any default values are specified for administrator login port (1100), DMZ Gateway port (44500), FTP banner message, or SFTP banner message, and will prompt you to change them. No default passwords, usernames, certificates, or keys are used.
  - When any unsecure protocols such as plaintext FTP or HTTP are detected; you are prompted to change them or present a compensating control.
  - The status of non-console (remote) access settings are in use and if SSL is not enabled. You are then given the option to either disable remote administration or enable SSL.
  - User login credentials persisted in memory beyond the absolute minimum time necessary (some configurations require this when reusing credentials for secondary connections)
  - Flood and DoS prevention settings set too low
  - FTP Anti-timeout prevention scheme disabled or FXP (site-to-site) permitted
- It is up to the administrator to determine whether an enabled protocol is necessary. No protocol is enabled by default.
- It is up to the administrator to remove any scripts, custom commands, Advanced Workflows or similar user-created files that are no longer in use.

Requirement 3: Protect Stored Account Data

- EFT provides a scheduled, automatic Clean-up Action. Deleted files can be purged by writing over the initial data using encrypted and/or pseudorandom data (PCI DSS 9.8). Disk quotas can be set to limit data storage.
- Encrypt PAN or other sensitive data using EFT's optional OpenPGP encryption module or third-party encryption utilities.
- EFT will detect and warn if Microsoft Encrypting File System (EFS) is being used.
- Access to keys through the administrator interface is limited to administrator roles with Site or Server access only.

- EFT will disallow creation of 512 or lesser certificate /key bit lengths. Default bit-length is set to 2048 bits for new keys. When importing SSL or SFTP keys, a warning will appear if a weak key is imported.

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

- Secure protocols such as SSL, TLS, and SFTP (SSH2) are provided for data transmission. Secure data transmission is enforced* by automatically redirecting incoming HTTP traffic to HTTPS.

Requirement 5: Protect All Systems and Networks from Malicious Software

- Requires measures external to EFT, such anti-virus software

Requirement 6: Develop and Maintain Secure Systems and Software

- Globalscape has formal processes for dealing with potential security vulnerabilities discovered in EFT, including an escalation process, a risk assessment that includes Common Vulnerability Scoring System (CVSS) risk ranking, and a process for notifying customers of critical patches or workarounds.
- The latest version of EFT is always available from the Globalscape website. Customers are automatically notified upon critical patch availability. It is up to the customer to install the patch within the designated one-month window.
- Globalscape takes a number steps to develop secure software, as documented here: https://kb.globalscape.com/KnowledgebaseArticle11061.aspx.
- Globalscape also performs routine third-party security scans of EFT's public-facing web interfaces as part of its quality assurance process.

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need-to-Know

- EFT provides complete control administrator and user access to resources, with administrator accounts completely segregated from user accounts
- Segregation and control of user access is achieved using unique accounts, permission groups, virtual folders, and settings templates Segregation and control of administrator access is accomplished via delegated, role-based administrator accounts.

Requirement 8: Identify Users and Authenticate Access to System Components

- EFT enforces unique usernames for both users and administrators, provides granular administrative controls over user provisioning and authorization, allows user and administrator account revocation, provides automatic removal of inactive users after 90 days, includes controls for temporarily enabling

/disabling users, auto-locks users after six failed login attempts , either for a period of time or permanently until the administrator unbans, and automatically expires sessions after 15 minutes of inactivity.

- EFT supports various combinations of password, certificate, two-factor, and public-key authentication mechanisms, secures passwords during transmission (assumes SSL or SSH), and storage (with a one way [uniquely salted] hash), verifies identity before allowing password reset or lost username retrieval according to OWASP guidelines, includes minimum length and a number of complexity options, expires and forces password change after 90 days, disallows password re-use, internal dictionary match, or username match, and can force first-time use password reset.
- Although EFT supports 2FA, this requirement is about network access, such as what is normally done over a VPN. You should disable remote (non-console) administrator access.
- The "Anonymous" password type is disallowed on a high-security-enabled Site. To comply, you will need to create unique accounts for service provider access, should there ever be a need to provide such access.
- EFT provides granular controls over which administrators can access EFT's reports from within the EFT Server console; however controls over access to the database (including the data itself) requires measures external to EFT.

Requirement 9: Restrict Physical Access to Cardholder Data

- EFT includes a data-wiping algorithm for sanitizing deleted data on disk.

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

- Preconfigured reports of all activity (including administrator actions*) within EFT can be generated on demand with the Auditing and Reporting Module (ARM).
- EFT will audit* all user access to data, and all administrator changes** to configuration settings. Access to audit trails, invalid logical access, authentication mechanisms, object creation, and initialization of audit logs is managed at the database server.
- EFT audits* user identity, type of transaction, date and time of transaction, transaction result, remote and local IP, and objects affected. *Requires ARM
- Audited data integrity depends on the chosen database solution and authentication architecture. EFT supports auditing to a central SQL or Oracle server.

- A daily PCI DSS Compliance report can be generated by EFT and sent via email to the appropriate recipient(s). Administrators can also attach any other canned or administrator created report to the daily email.
- EFT logs and reports audit EFT-specific systems; auditing of other network systems requires measures external to EFT.

Requirement 11: Test Security of Systems and Networks Regularly

- Requires measures external to EFT.

Requirement 12: Support Information Security with Organizational Policies and Programs

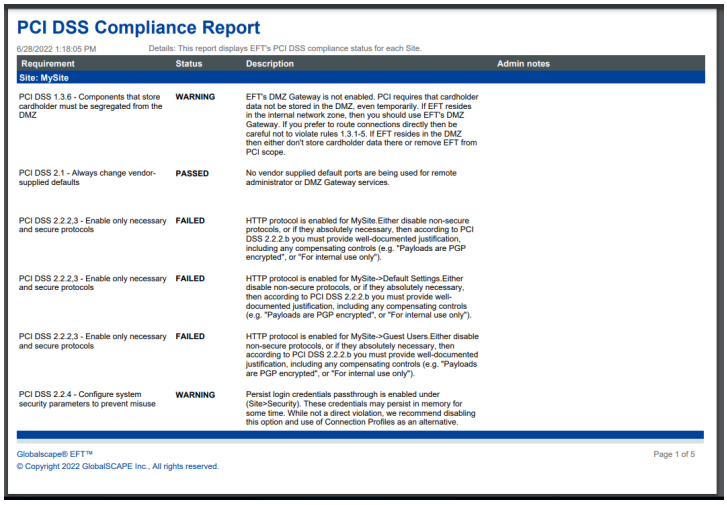
- Requires measures external to EFT

PCI DSS Compliance Report

The RCM module includes the ability to audit EFT for compliance with the PCI DSS requirements. EFT scans all PCI DSS requirements addressed in EFT, and then reports on the compliance status of each requirement (Pass, Fail, or Warning). The report also provides a description of the requirement tested for each item. For failed requirements, the report presents a reason the non-compliant setting was used, if you provided one at the time that particular setting was disabled/changed.

To generate the PCI DSS Compliance report

- To generate the report in real time, do one of the following:
  - On the main menu, click **Report >PCI DSS Compliance Report**. A PCI DSS Compliance report is generated for each Site.
  - In the Site's **Event Rule** node, click **Report Event**. In the right pane, click **Run Now**. The report is emailed to the email address defined in the Rule.
- To generate the report on a recurring schedule, define a Scheduler Timer Event Rule with the Generate Report Action. In the Event Rule, you can define whether to email the report and/or save the report to a file. A report is generated specific to the Site on which the Event Rule is configured.



PCI DSS Compliance Report

6/28/2022 1:18:05 PM Details: This report displays EFT's PCI DSS compliance status for each Site.

Requirement	Status	Description	Admin notes
Site: MySite			
PCI DSS 1.3.6 - Components that store cardholder must be segregated from the DMZ	WARNING	EFT's DMZ Gateway is not enabled. PCI requires that cardholder data not be stored in the DMZ, even temporarily. If EFT resides in the internal network zone, then you should use EFT's DMZ Gateway. If you prefer to route connections directly then be careful not to violate rules 1.3.1-5. If EFT resides in the DMZ then either don't store cardholder data there or remove EFT from PCI scope.	
PCI DSS 2.1 - Always change vendor-supplied defaults	PASSED	No vendor supplied default ports are being used for remote administrator or DMZ Gateway services.	
PCI DSS 2.2.2,3 - Enable only necessary and secure protocols	FAILED	HTTP protocol is enabled for MySite.Either disable non-secure protocols, or if they absolutely necessary, then according to PCI DSS 2.2.2.b you must provide well-documented justification, including any compensating controls (e.g. "Payloads are PGP encrypted", or "For internal use only").	
PCI DSS 2.2.2,3 - Enable only necessary and secure protocols	FAILED	HTTP protocol is enabled for MySite->Default Settings.Either disable non-secure protocols, or if they absolutely necessary, then according to PCI DSS 2.2.2.b you must provide well-documented justification, including any compensating controls (e.g. "Payloads are PGP encrypted", or "For internal use only").	
PCI DSS 2.2.2,3 - Enable only necessary and secure protocols	FAILED	HTTP protocol is enabled for MySite->Guest Users.Either disable non-secure protocols, or if they absolutely necessary, then according to PCI DSS 2.2.2.b you must provide well-documented justification, including any compensating controls (e.g. "Payloads are PGP encrypted", or "For internal use only").	
PCI DSS 2.2.4 - Configure system security parameters to prevent misuse	WARNING	Persist login credentials passthrough is enabled under (Site>Security). These credentials may persist in memory for some time. While not a direct violation, we recommend disabling this option and use of Connection Profiles as an alternative.	

Globalscape® EFT™ Page 1 of 5

© Copyright 2022 GlobalSCAPE Inc., All rights reserved.

For a description of each PCI DSS requirement covered in the report, refer to How PCI DSS Requirements Addressed.

For details of generating reports, refer to Generating a Report.

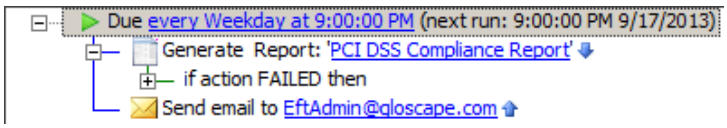
Related Topics

- Warnings for HS Violations
- PCI DSS Requirements

- Possible PCI DSS Compliance Report Outcomes
- Introduction to Event Rules
- Defining Event Rules
- Scheduler (Timer) Event
- Generate Report Action

Automating the Compliance Report

When you create a high security-enabled Site, EFT creates a Report Event Rule automatically. The **Report Event** Rule generates a PCI DSS Compliance Report once per week using the Generate Report Action. The report is converted to HTML and then emailed using the Send notification email Action and the %FS.REPORT_CONTENT% variable. You can edit the Rule to specify when to generate the report and to whom to send the report.



Optionally, you can run the PCI DSS Compliance Report "on the fly" by clicking **Reports > Run PCI DSS Compliance Report** on the administration interface main menu. If the Regulatory Compliance Module (RCM) is not activated, the PC DSS Compliance Report is not available.

PCI DSS Possible Compliance Report Outcomes

The PCI DSS Compliance Report displays the requirement name, status (PASSED, FAILED, WARNING), description of the requirement, notes that you typed in the Warning box (explanation, justification, or compensating control), report name, and date the report was generated, and description of the report. The report is grouped by and sorted by PCI DSS Requirement.

If the report is generated after the trial has expired, the report contains a statement stating that the module has expired instead of the standard report.

When in trial or after the module is activate, the report contains the following information:

The status of audited PCI DSS requirements appears in the report.

- 1.x – DMZ Gateway disabled or no connectivity
- 2.x – Remote administrator enabled by not secure, vendor defaults in use, insecure protocols in use (FTP, HTTP) or insecure settings (NOOP and FXP), auto-ban/flood detection set too low or disabled, and login credential persistence enabled.
- 3.x – Disk quotas not present for limiting storage amounts, missing clean-up rule for data retention and disposal compliance.
- 4.x – Weak cryptography in use (SSL version, cipher strength, manually specified ciphers, weak HMACs), insecure settings such as SSL clear command clear data channel in use.
- 5.x – No checks
- 6.x – No checks
- 7.x – Presence of more than one full-control administrator account
- 8.x – Password length or complexity not enforced, password reuse allowed, idle session timeout disabled or set to high, inactive accounts not disabled or removed after 90 days, failed logins not resulting in account lockout after six (or less) attempts, password reset not allowed, password reset not forced on initial login, anonymous accounts present, and passwords not expiring after 90 days or sooner.
- 9.x – Secure wiping of deleted data not enabled
- 10.x – ARM not enabled or no connectivity

- 11.x – No checks
- 12.x – No checks

Refer to How EFT Addresses PCI DSS Requirements for details of each requirement.

Warnings for PCI DSS Violations

When EFT warns you of a non-compliant setting, if you do not specify a setting that meets the PCI DSS requirement, you can specify the compensating controls (hardware, software, or policy) you are using to satisfy the requirement. The information that you provide in the warning message appears in the PCI DSS Compliance Report, which you can provide to Qualified Security Assessors (QSAs) or Approved Scanning Vendors (ASVs), individuals who are certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS requirements.

For Sites created using the "strict security settings" option, if you attempt to change a setting that would cause EFT to no longer meet PCI DSS requirements, when you click **Apply** to save the changes on EFT, EFT does not commit the change, and a warning message appears that describes one or more violations.

If you do not activate the Regulatory Compliance Module (RCM), this feature is disabled when the trial has expired.

For each violation identified in the **PCI DSS Violations** dialog box, you can accept the non-compliant setting (**Apply this change anyway**) and provide a reason for accepting each setting (for example, if you are using an alternate solution) or you can discard the change (**Don't apply this change**). If you accept the change and provide a reason, the warning and the reason that you provided appear in the PCI DSS Compliance Report.

Related settings are audited and reported on as a group (for example, all of the SSL-related settings or all of the account-related settings). For example, suppose that on Monday you disable the account lockout settings for a user and specified in the PCI DSS Violations dialog box your reason for allowing this non-compliant setting. Then on Wednesday, you change a complex password setting. The **PCI DSS Violations** dialog box appears and displays both of these settings, as well as others for which you provided a reason, and you will be required to allow the change and specify a reason or discard the changes for each of the non-compliant settings before EFT commits the changes. (That is, the allow or discard flag is separate, but they are audited and reported on as a group.) This functionality is designed to remind you of the non-compliant settings in case you want to bring them into compliance in EFT.

If PCI DSS Violations are detected

1. Click a violation in the list, then do one of the following for each of the violations listed:

    - If you want to correct the violation, click **Don't apply this change**, click **Continue**, correct the setting, and then click **Apply**.
    - If you want to keep the non-compliant setting, click **Apply this change anyway**, then in the **Provide justification and describe compensating control** box, type the reason for keeping the non-compliant setting. The description will appear in the PCI DSS Compliance report.
2. Click **Continue**. You must address each violation in the list before you can click **Continue**.

Reporting of failed items occurs at the highest level of failure only, except in the case of an explicit setting that violates compliance. For example:

- If a Site failed compliance because **Enforce strong (complex) passwords** was disabled (check box cleared), the report is generated for the entire Site.
- If **Enforce strong (complex) passwords** was enabled for the Site, but was disabled for a Settings Template, the report is generated for the Settings Template.
- If **Enforce strong (complex) passwords** was enabled for the Site and Settings Template, but disabled for some users, EFT reports for each of those users.
- If **Enforce strong (complex) passwords** was disabled for the Site, enabled for the Settings Template, and disabled for a user, the warning appears for the Site violation *and*for the user account that is in violation.

EFT stores PCI DSS compensating controls information provided in its auditing database (ARM). If ARM is disabled, violations are still identified in the report; however, the justifications that you type when you accept a non-compliant setting are not recorded in the database. You can still run the report, but the justifications that you provide will not appear in the report. When settings are changed via the COM API that violate PCI DSS compliance, EFT will reject the change and return the error code "error 53."

Remote Agent Module

The topics in this section provide information about and procedures for using Remote Agents.

- Introduction to Remote Agents
- Installing Remote Agents
- Decommissioning a Remote Agent
- Managing Remote Agents
- Remote Agent Templates
- Remote Agents License Status
- Remote Agent Updates
- Remote Agent Event Rules
- Remote Agent Context Variables
- Remote Agent Logging
- Remote Agents in the VFS
- Sending Files (Offloading) to a Different Server

Introduction to Remote Agents

The Remote Agent Module (RAM) provides centralized control for automating transactions from distributed systems. RAM enables automatic interactions between branch offices, point-of-sale terminals, business partners, field agent laptops, or other remote systems and your EFT server residing in a central location.

Install the *Remote Agent* service at the remote location, then enable the agent to process files that arrive in a monitored “hot” folder, or retrieve or send files to EFT on a schedule. Remote Agents call home routinely to gather updated instructions, removing the need for administrators to deploy and manage automation scripts manually at each branch office or remote location. RAM provides much of the power of EFT Event Rules in a package that takes just a few megabytes of space and can be deployed in seconds.

Remote Agents can be defined regardless of authentication method used on the Site, and leverages the Site's security settings, including transfer speed, and socket connection. Remote Agent connection is allowed only over HTTPS.

For every connection, the Agent's and Site's banned IPs list and client SSL certificate is checked. EFT fails the authentication attempt if the certificates do not match.

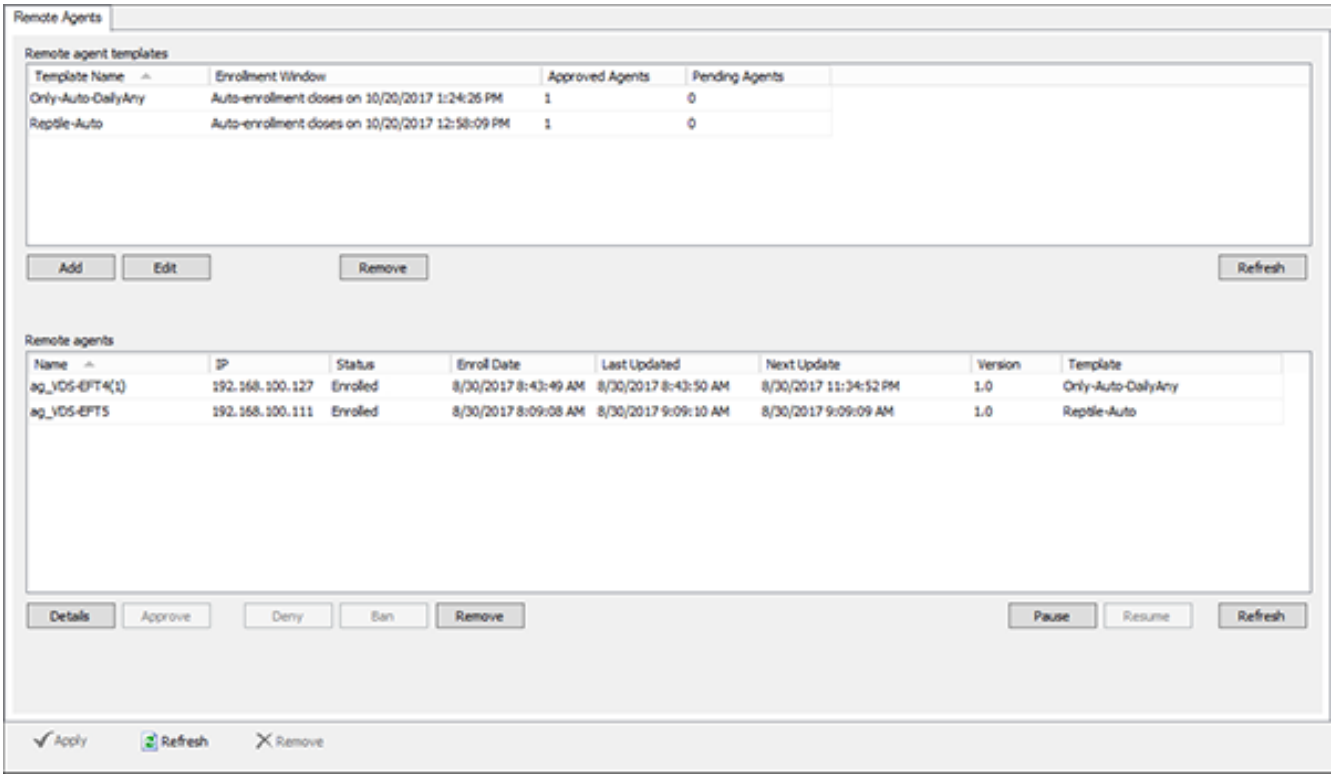
- There are no administrator, user, or client connections at the Remote Agent end of the connection.
- The Remote Agent connection is "headless," meaning there is no interface.
- Users place files in a directory on their system and Folder Monitor picks it up or processes it based on a schedule

IMPORTANT: To install Agents, you must have sufficient administrator privileges to the Remote Agent computer’s installation and configuration folders.

Each Remote Agent:

- Receives the initial rule set assigned to it, along with API key (GUID), certificates, etc.
- Calls home periodicallyto receive updated rule sets (that is, gets new orders)
- Rules are triggered by EFT Timer and Folder Monitor logic; rules can push/pull files to the "home office" only

EFT displays interaction between end points and the central hub, captures interaction of Remote Agents when requesting updated instructions, and allows administrators to easily add, modify, and remove Remote Agents and templates.



Installing Remote Agents

Requirements for installation

- To install Agents you must have sufficient administrator privileges to the Agent's installation and configuration folders.
- Operating systems supported on RAM computers: Windows Server 2022, 2019, and 2016, Windows 10/ 11.
- HTTP/HTTPS module
- SSL must enabled and available on port 443
- Visual C++ and Redistributable for Visual Studio (for installation).
- EFT server must be registered
- After installation, the computer may require a reboot.

If prerequisites are not installed (includes installer wizard):

EFTRemoteAgentBundle.exe, a bootstrapper package in **..\ProgramData\Globalscape\EFT Server\RemoteAgent** (or the **..\<HA_share>\Remote Agent** folder on the EFT computer), contains the MSI file, verifies and installs the prerequisites and the application. You can run the EFTRemoteAgentBundle.exe and manually input the host, port, and template ID. The EXE file has an installer wizard in which you input the host, port, and Template ID. You can still use the EFTRemoteAgentBundle.exe if the prerequisites are installed.

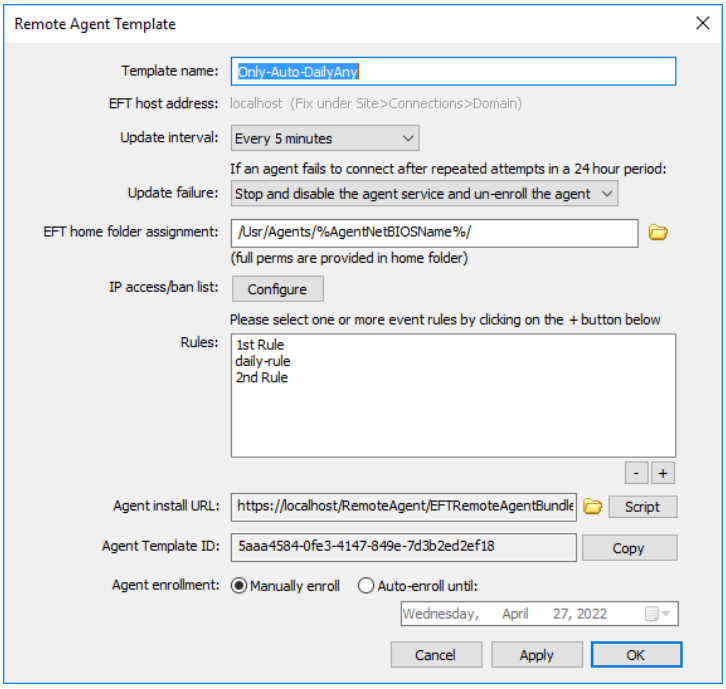
> **NOTE:** The script URL for downloading EFTRemoteAgentBundle.exe can be found in the Remote Agent Template interface in EFT, **..\ProgramData\Globalscape\EFT Server\RemoteAgent**, and **..\<HA_share>\Remote Agent** on the EFT computer.

If prerequisites already installed (silent installation):

The EFTRemoteAgent.msi file does **not** contain the prerequisites. The EFTRemoteAgent.msi is mainly used for System Center Configuration Manager (SCCM), group policy deployment, or if you want a silent installation.

To install the Remote Agent

1. The EFT administrator should make the EXE available to download via WTC or a shared Workspace by creating a Remote Agent Template.



2. On the Remote computer, log in to the WTC and download **EFTRemoteAgentBundle.exe**.
3. The Remote Agent can be installed at command line using the default script **in the folder in which you downloaded the EXE.** Ensure that the EXE is in the same directory as you run the script.

   ```
   EFTRemoteAgentBundle.exe /s acceptEula="yes"
   host="localhost" port=443 tid="075a9515-7861-4ecc-b56a-
   02d1e6c0cd25" AUTODETECTPROXY=false
   ```

   The script completes the host, port, and agent template ID (tid) fields (as shown in the script and in the Remote Agent Template in EFT).

4. After the Agent is installed, you will need to create at least one Agent rule.

Manual Installation

For manual installations (below), the EFT administrator will have to provide the EFT host address, port, and Template ID so that you can enter the information manually.

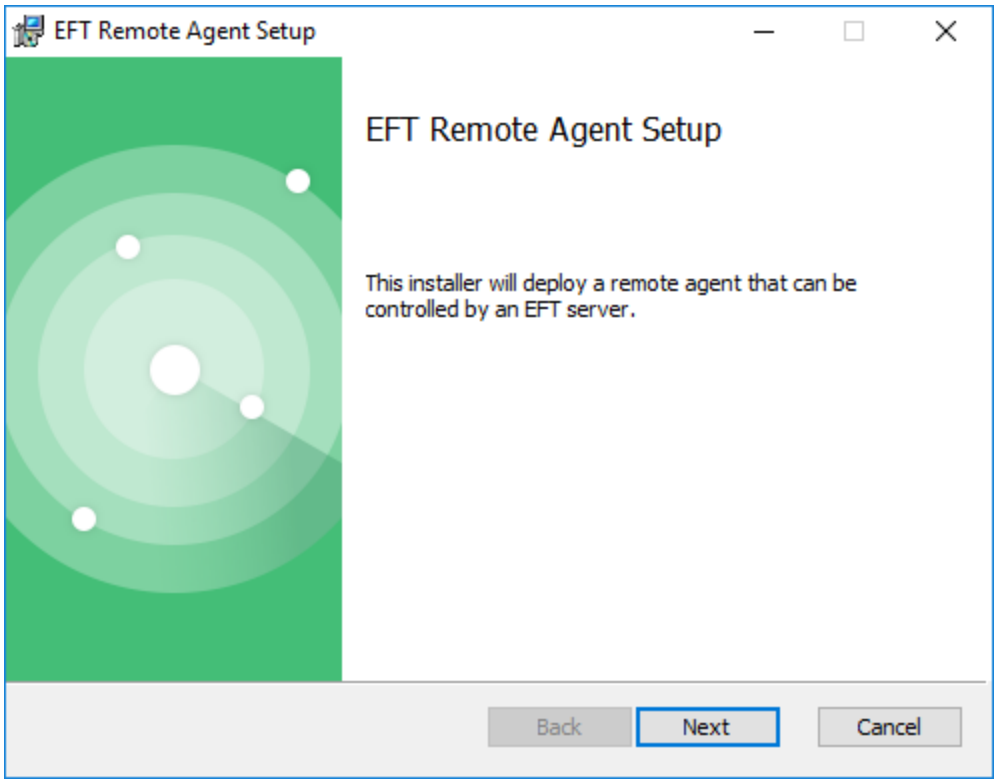
USE THE PROCEDURE BELOW FOR MANUAL INSTALLATION IF YOU CAN'T USE THE SCRIPT DESCRIBED ABOVE

To install the Remote Agent Bundle

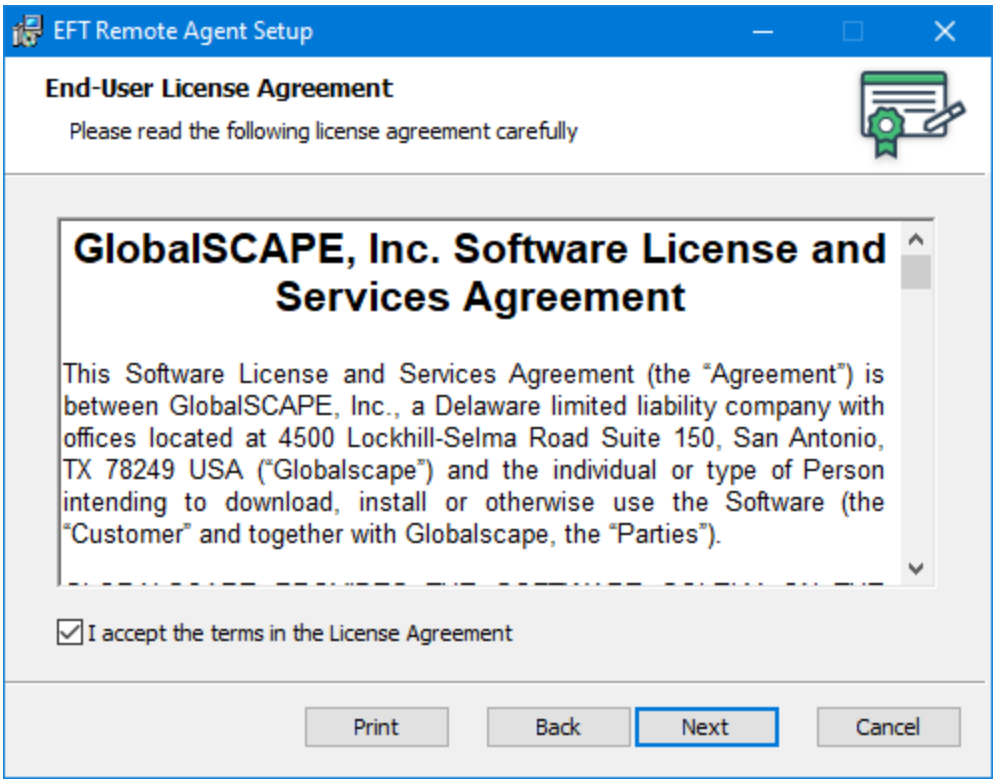
1. Before beginning installation, be sure you have the host address, port number, and agent template ID (tid) shown in the Remote Agent Template in EFT.
2. On the computer on which the Remote Agent is to be installed, run the installer in **\ProgramData\Globalscape\EFT Server\RemoteAgent**. The **Remote Agent Bootstrapper** installer wizard appears.

   The bootstrapper checks for and installs prerequisites, if not already installed, then launches the Remote Agent installer wizard.

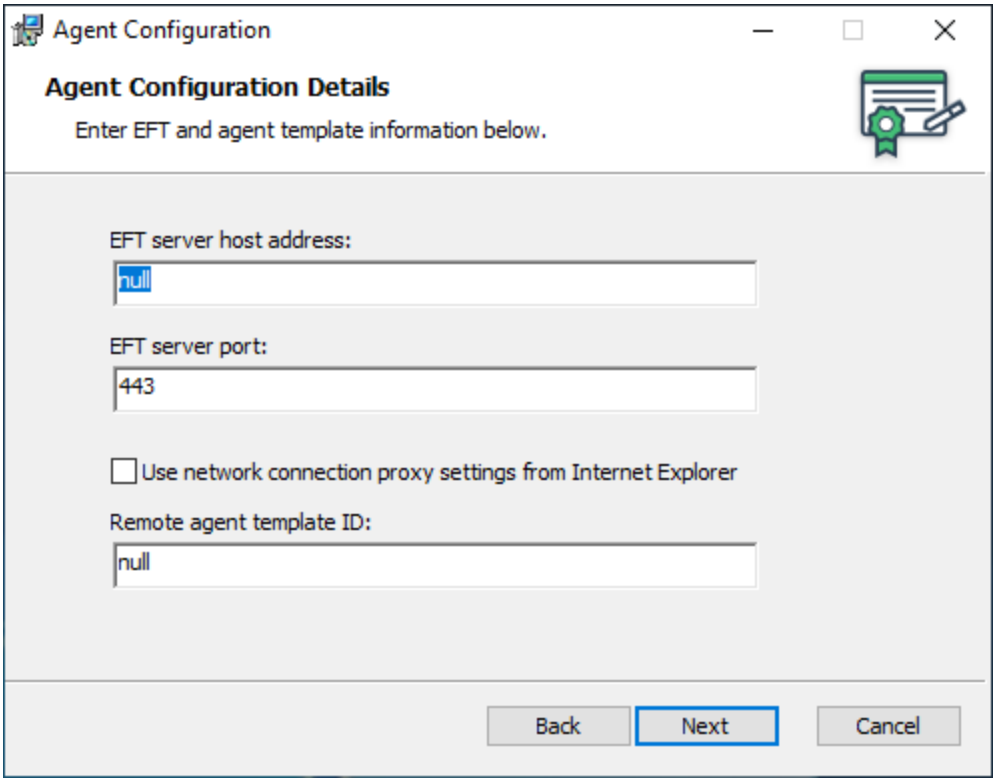
3. Click **Install**. The installer appears.



4. Click **Next**. The **End-User License Agreement** page appears.



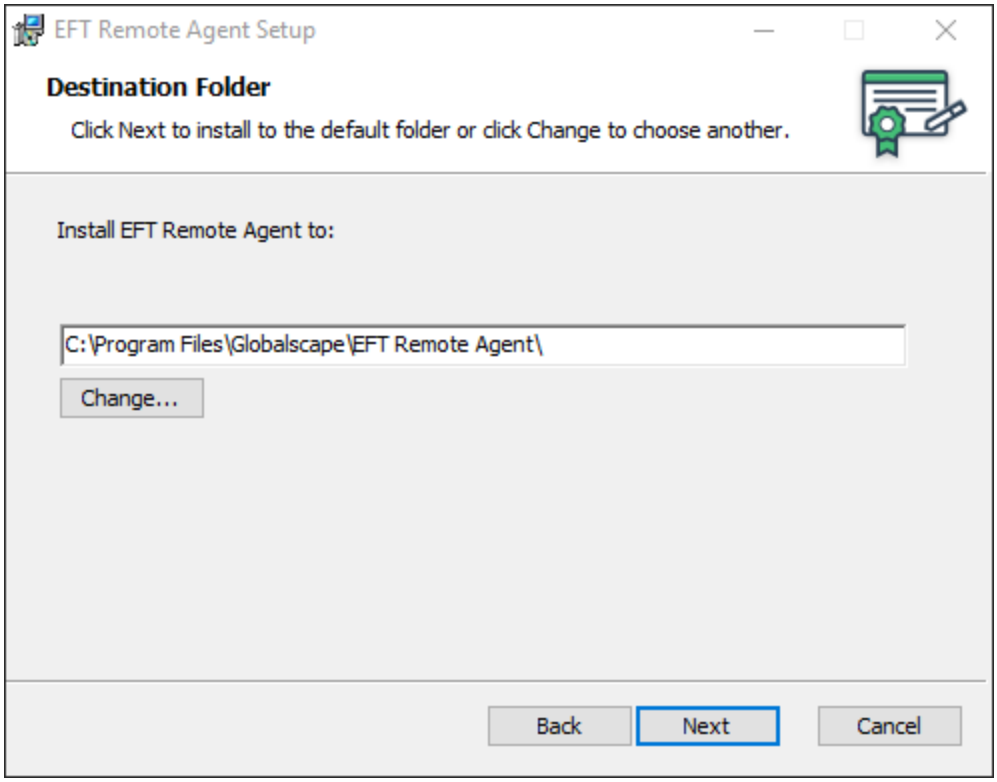
5. Select the check box, then click **Next**. The **Configuration** screen appears.



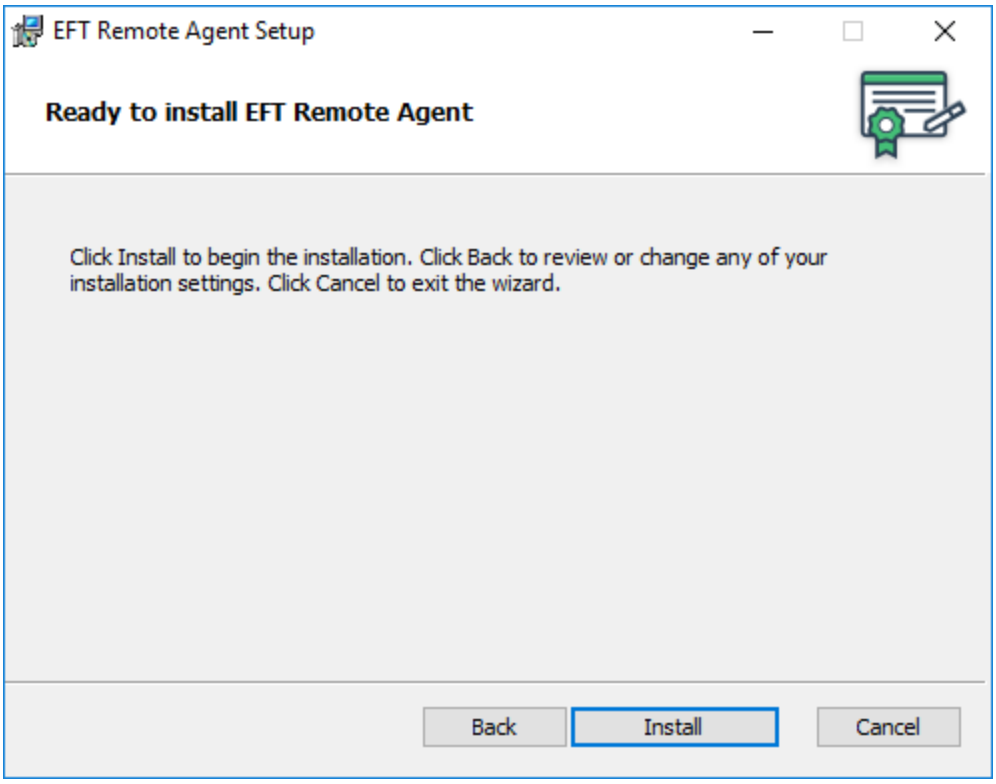
6. If you are running the installer manually (not from a script) you must provide the EFT server host address, EFT server port, and Remote agent template ID. (The EFT administrator can provide you these from the Remote Agent Template as show in the script procedure above.)
7. Select the **Use network connection proxy settings from Internet Explorer** check box to use the system's default proxy settings (that is, the configuration in Internet Explorer under **Internet Options > Connections tab > LAN settings** for proxy, which is used by all apps that require Internet access).

   > **NOTE:** Event rules configured with a proxy will use that proxy even if autodetect is enabled when Remote Agent is installed (can be changed if needed). The "Silent install" URL is:
   > `EFTRemoteAgentBundle.exe /s accepteula=yes host="localhost" port=443 tid="a247515e-396c-4932-a67a-d342363fc45c" AUTODETECTPROXY=false`

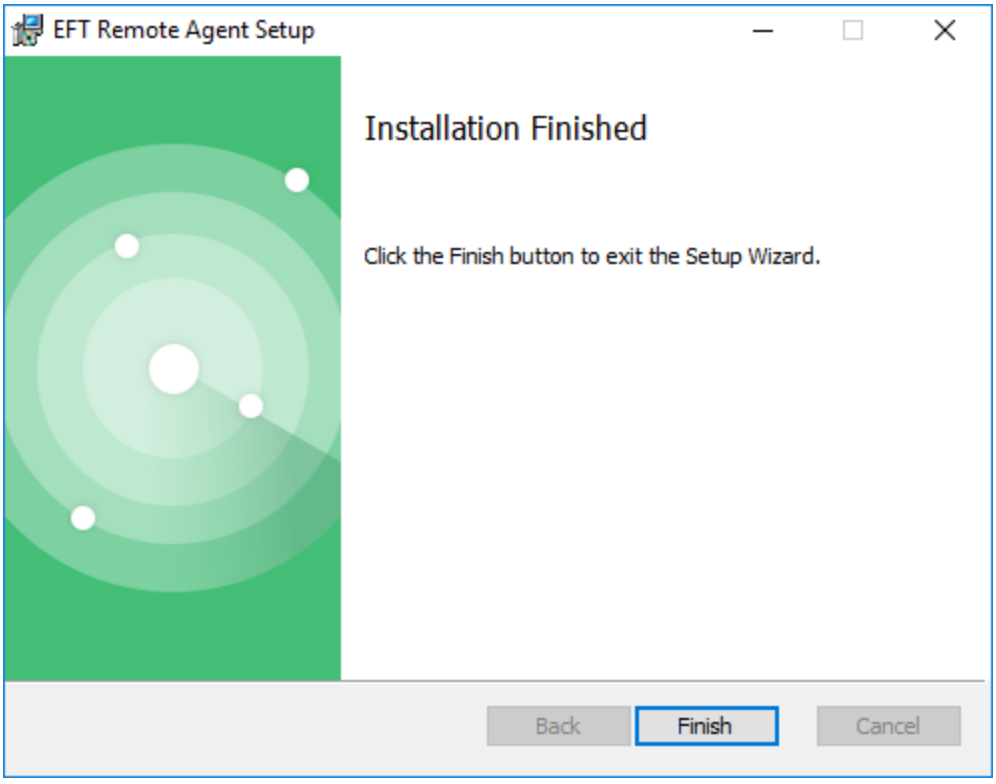
8. Click **Next**. The **Destination Folder** screen appears.



9. By default, the Remote Agent is installed in **C:\Program Files\Globalscape\EFT Remote Agent**. If you want to install in a different location, click **Change**.
10. Click **Next**. The **Ready to install** screen appears.



11. Click **Install**. The **Finished** screen appears.



12. Click **Finish**.
13. Click **Close**to exit the installer.

On the EFT computer, under the **Remote Agents** node, you will see the Remote Agent connect to EFT. If manual enrollment is specified, you will need to click the Remote Agent in the list, then click **Approve**. You may have to wait for the next update to see a change in status.

Next step: Create a Remote Agent Event Rule

Remote Agent Updates

Each Remote Agent receives the initial rule set assigned to it, along with API key (GUID), certificates, etc. from its assigned template. After the Remote Agent enrolls itself with EFT, it then calls home periodically to receive updated rule sets (that is, gets new orders). This topic describes that process.

> **NOTE:** When upgrading from EFT v8.1 to 8.2, during the upgrade state, the remote agent will not trigger any event rules until the upgrade has completed. The time to complete the upgrade is based on the update interval defined in the template. As a workaround to speed up this process, you could change the Remote Agent Template update interval to a shorter time, such as near real-time, once a minute, or every 5 minutes prior to upgrading. Then once the upgrade is complete, update the interval again to its initial value.

Automatic Upgrades

- If the agent determines that the agent installer version (on disk) being advertised by EFT is different than its own version, the agent will download and run that installer (auto-upgrade)
- Agents will log their update process including any errors
- EFT will log from its perspective when it detects an agent update occurred, including any errors detected or provided by the agent
- EFT's installer will backup prior agent installers when performing a general (EFT) upgrade
- Agent update process only occurs for enrolled active or enrolled paused agents, but not pending enrollment or pending removal agents.
- Only agents that support auto-update will be able to update to a newer version. Agents installed prior to EFT v7.4.7 will not have this functionality.
- Failure to download the new agent installer will result in a logged failure and the agent will retry again on its next call home.
- After successfully downloading the new agent installer, if an agent fails to spawn the process to run the new installer, the agent will log and take itself offline.

Enrolled remote agents will call home to obtain updated orders at agent service startup and at the defined update interval set obtained at enrollment for that agent template.

- Near real time - The Agent will check for updates every 15-30 seconds.
- Every 5 minutes - The Agent will check for updates every 5 minutes.

- Every 30 minutes - The Agent will check for updates every 30 minutes.
- Hourly - The Agent will check for updates every 60 minutes. The start timer is based on service start time (+60 minutes and repeat)
- Daily - The Agent will check for updates randomly any time of the day and repeat daily at that same time
- Daily - afterhours - The Agent will check for updates randomly between 11PM and 6AM local time and repeat nightly at same the time.
- Time zones are with respect to the Agent's location
- For manual updates, "update now"

If the Remote Agent fails to connect to EFT to receive updated instructions:

EFT allows a "grace period before failure" of one day for all update intervals. Below is an example of what happens when a failure occurs:

1. The agent logs a temporary update failure.
2. The agent tries again in 5 minutes, then 15 minutes, then 30 minutes. (These attempts will occur only for hourly and daily options.)
3. After 1 day of re-trying, the agent logs a failed update and then performs the specified option for update failure described below.
4. On the next scheduled update cycle, the agent will try to connect to EFT again.
5. If the agent service is restarted, the agent will repeat the connection process above.

If an Agent fails to connect to EFT after repeated attempts in a 24-hour period, one of three actions can take place, as specified by the EFT administrator:

- Stop and disable the agent service and un-enroll the agent
- Stop and disable the agent service
- Stop the agent service only.

If the agent is unable to connect after two entire update cycles, the agent will:

1. Log "critical failure to update."
2. Take itself offline (service stop)
3. Set its service to disabled.
4. Not reset itself to the pre-enrollment state.

If the agent fails to authenticate when attempting to update its instructions (authentication or certification failure):

1. The agent will log the authentication failure(s)
2. The agent will try again in 5 minutes, then 15 minutes, then 30 minutes.
3. Once all retries are exhausted, the agent will log a failed update, then reset itself to pre-enrollment state. (Resetting itself provides an opportunity for administrator to forcibly remove enrolled agents from EFT.)
4. The agent will agent will bring itself offline (service stop), as there is no point in trying again or to keep rules active if unable to authenticate.
5. The agent will set its service to disabled.
6. If the agent service is restarted, the enrollment process will occur again.

If the agent successfully connected and authenticated:

1. The agent will communicate its agent version to EFT.
2. The agent will obtains its update interval, based on the agent's parent template.
3. The agent will obtain its designated list of rules associated with that agent, based on the agent's parent template
4. The agent and EFT will exchange when next call home will occur
5. The agent will obtain status information from EFT:
    - Whether agent should suspend (pause) its rules until further notification
    - Whether agent should re-activate (resume) its rules
6. EFT updates the last called home and next call home times in the agent list

If the agent service is ever stopped (regardless of how/why),

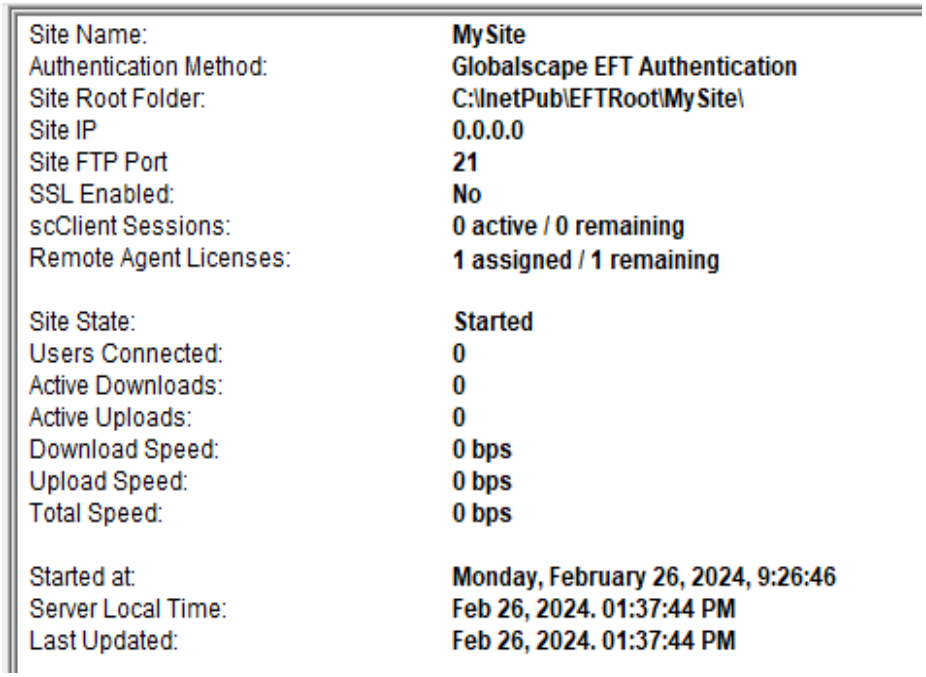
- The ruleset and update interval is lost.
- When the agent service is started, it will call home and obtain updated orders.

When an agent is removed, that agent is unknown to EFT; all records of that agent's existence are removed. After a certain number of failed authentication attempts, the agent will essentially un-enroll itself and take itself offline.

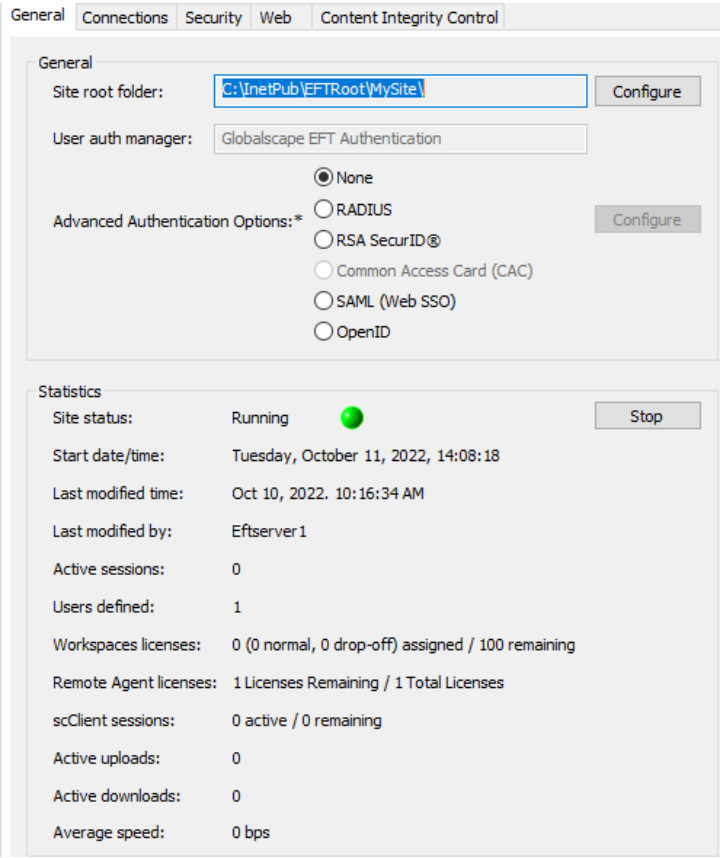
Remote Agents License Status

Each Remote Agent uses one Client Access License (CAL), whether the Agent is paused (disabled) or active. Removing an agent releases the CAL back to the pool of licenses available. New agents cannot be provisioned more than the number of CALs licensed. That is, if you have 5 Remote Agent CALs, you can only create 5 Remote Agents. In trial mode, you can only define up to 10 Remote Agents.

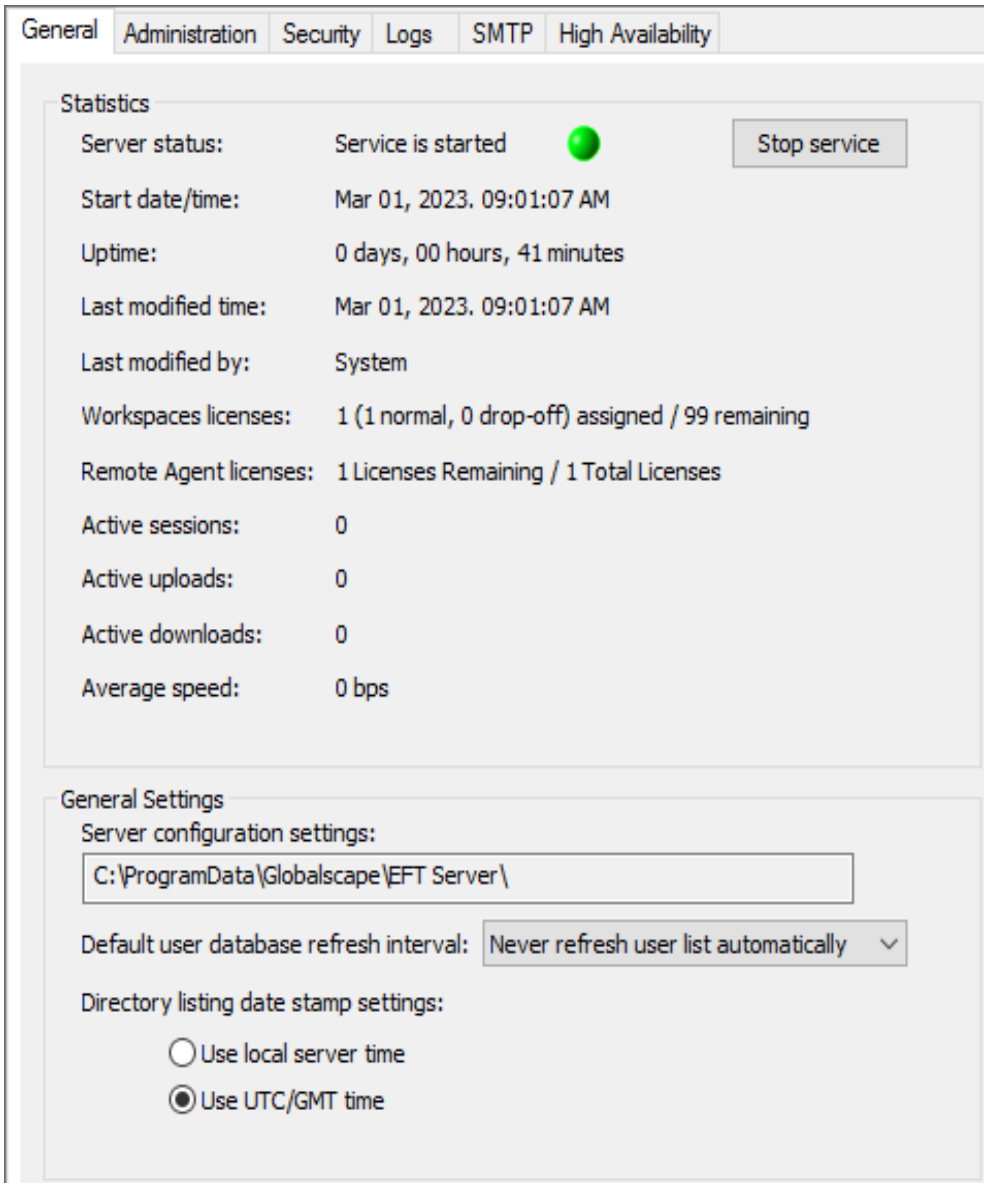
The Remote Agents license (RAM licenses) status can be viewed in the EFT administration interface, on the **Status** tab's **Site**node:



And on the **Server** tab > **Site** node > **General**Tab:



And on the **Server** tab > **Server** node > **General**tab:



Remote Agent Updates

Each Remote Agent receives the initial rule set assigned to it, along with API key (GUID), certificates, etc. from its assigned template. After the Remote Agent enrolls itself with EFT, it then calls home periodically to receive updated rule sets (that is, gets new orders). This topic describes that process.

> **NOTE:** When upgrading from EFT v8.1 to 8.2, during the upgrade state, the remote agent will not trigger any event rules until the upgrade has completed. The time to complete the upgrade is based on the update interval defined in the template. As a workaround to speed up this process, you could change the Remote Agent Template update interval to a shorter time, such as near real-time, once a minute, or every 5 minutes prior to upgrading. Then once the upgrade is complete, update the interval again to its initial value.

Automatic Upgrades

- If the agent determines that the agent installer version (on disk) being advertised by EFT is different than its own version, the agent will download and run that installer (auto-upgrade)
- Agents will log their update process including any errors
- EFT will log from its perspective when it detects an agent update occurred, including any errors detected or provided by the agent
- EFT's installer will backup prior agent installers when performing a general (EFT) upgrade
- Agent update process only occurs for enrolled active or enrolled paused agents, but not pending enrollment or pending removal agents.
- Only agents that support auto-update will be able to update to a newer version. Agents installed prior to EFT v7.4.7 will not have this functionality.
- Failure to download the new agent installer will result in a logged failure and the agent will retry again on its next call home.
- After successfully downloading the new agent installer, if an agent fails to spawn the process to run the new installer, the agent will log and take itself offline.

Enrolled remote agents will call home to obtain updated orders at agent service startup and at the defined update interval set obtained at enrollment for that agent template.

- Near real time - The Agent will check for updates every 15-30 seconds.
- Every 5 minutes - The Agent will check for updates every 5 minutes.

- Every 30 minutes - The Agent will check for updates every 30 minutes.
- Hourly - The Agent will check for updates every 60 minutes. The start timer is based on service start time (+60 minutes and repeat)
- Daily - The Agent will check for updates randomly any time of the day and repeat daily at that same time
- Daily - afterhours - The Agent will check for updates randomly between 11PM and 6AM local time and repeat nightly at same the time.
- Time zones are with respect to the Agent's location
- For manual updates, "update now"

If the Remote Agent fails to connect to EFT to receive updated instructions:

EFT allows a "grace period before failure" of one day for all update intervals. Below is an example of what happens when a failure occurs:

1. The agent logs a temporary update failure.
2. The agent tries again in 5 minutes, then 15 minutes, then 30 minutes. (These attempts will occur only for hourly and daily options.)
3. After 1 day of re-trying, the agent logs a failed update and then performs the specified option for update failure described below.
4. On the next scheduled update cycle, the agent will try to connect to EFT again.
5. If the agent service is restarted, the agent will repeat the connection process above.

If an Agent fails to connect to EFT after repeated attempts in a 24-hour period, one of three actions can take place, as specified by the EFT administrator:

- Stop and disable the agent service and un-enroll the agent
- Stop and disable the agent service
- Stop the agent service only.

If the agent is unable to connect after two entire update cycles, the agent will:

1. Log "critical failure to update."
2. Take itself offline (service stop)
3. Set its service to disabled.
4. Not reset itself to the pre-enrollment state.

If the agent fails to authenticate when attempting to update its instructions (authentication or certification failure):

1. The agent will log the authentication failure(s)
2. The agent will try again in 5 minutes, then 15 minutes, then 30 minutes.
3. Once all retries are exhausted, the agent will log a failed update, then reset itself to pre-enrollment state. (Resetting itself provides an opportunity for administrator to forcibly remove enrolled agents from EFT.)
4. The agent will agent will bring itself offline (service stop), as there is no point in trying again or to keep rules active if unable to authenticate.
5. The agent will set its service to disabled.
6. If the agent service is restarted, the enrollment process will occur again.

If the agent successfully connected and authenticated:

1. The agent will communicate its agent version to EFT.
2. The agent will obtains its update interval, based on the agent's parent template.
3. The agent will obtain its designated list of rules associated with that agent, based on the agent's parent template
4. The agent and EFT will exchange when next call home will occur
5. The agent will obtain status information from EFT:
    - Whether agent should suspend (pause) its rules until further notification
    - Whether agent should re-activate (resume) its rules
6. EFT updates the last called home and next call home times in the agent list

If the agent service is ever stopped (regardless of how/why),

- The ruleset and update interval is lost.
- When the agent service is started, it will call home and obtain updated orders.

When an agent is removed, that agent is unknown to EFT; all records of that agent's existence are removed. After a certain number of failed authentication attempts, the agent will essentially un-enroll itself and take itself offline.

Remote Agent Templates

In EFT, a Remote Agent template stores configuration and rules that can be shared by many Agents, and an installer script is generated for each Remote Agent template. Therefore, if one or more remote offices have one set of needs, and another set of remote offices has different needs, a separate remote agent template will distinguish between both sets of offices, allowing you to control each group separately.

In addition to creating templates on this tab, you can monitor when Remote Agents have requested enrollment, are approved, denied, awaiting approval, or decommissioned, and information about the Remote Agents such as IP address, status, enrollment date, and dates when it was updated. The tab also provides options to deny, ban, or remove the agent, and pause and resume remote Agent rules.

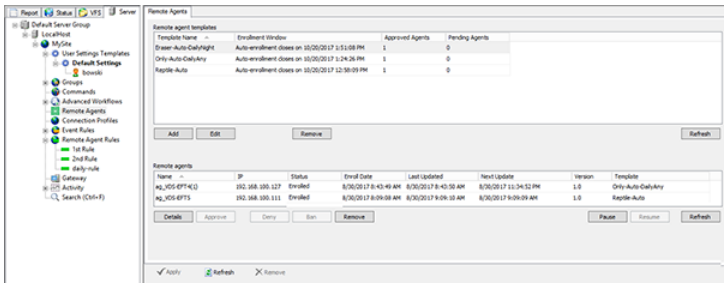
Before creating your first Remote Agent Template, you should define a Remote Agent Event Rule. If you haven't created any Remote Agent Event Rules, you can still create the template, but then you'll have to edit the template after you create the Event Rule to add the Event Rule to the template.

Ensure that HTTPS is allowed on the port specified and that it is not being blocked by the Windows firewall at either end of the connection.

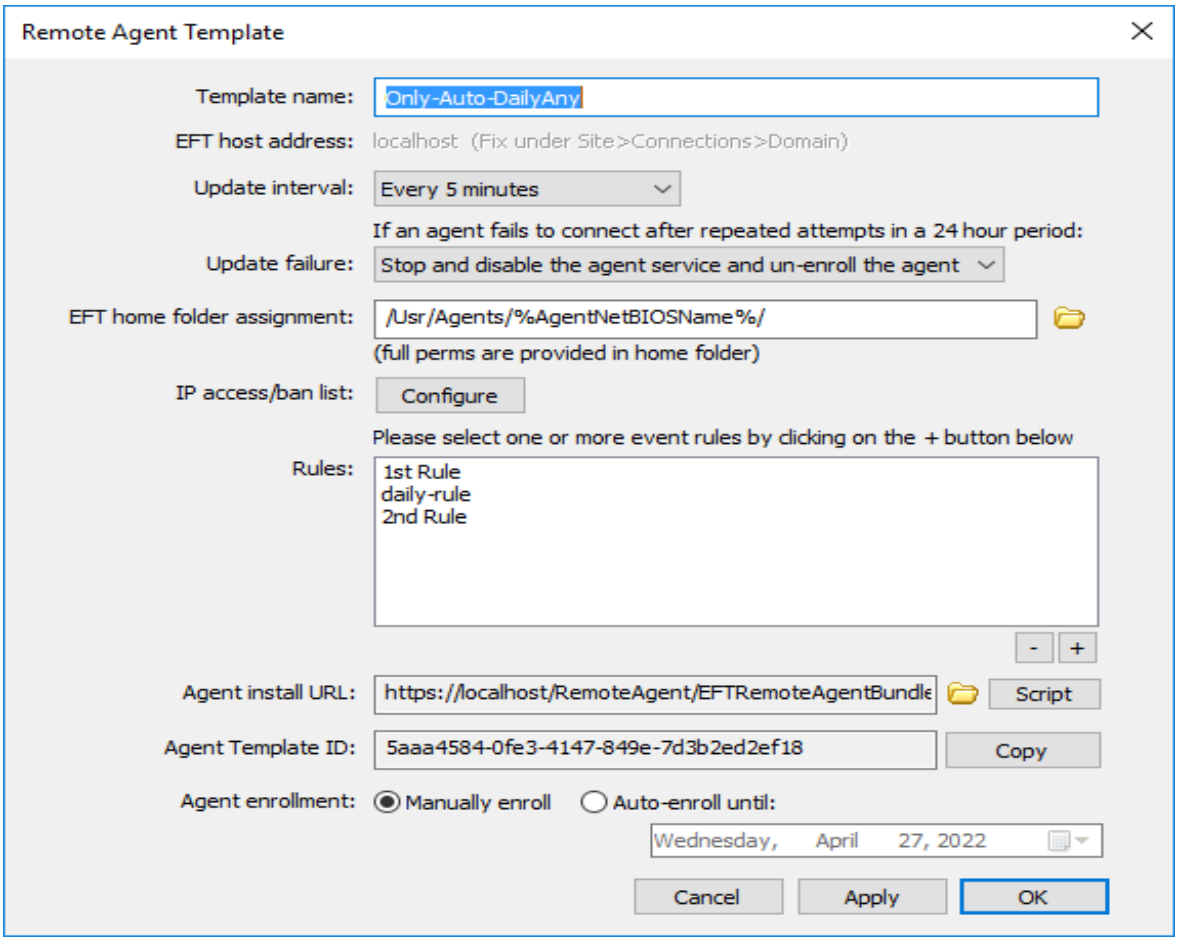
> **NOTE:** You must add a Remote Agent rule to the template for the template to be active. If you don't add a Remote Agent rule, the ARM report will show a successful event for the Remote Agent, even though nothing was triggered.

To create a new Remote Agent template

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, expand the Site node, then click **Remote Agents**.

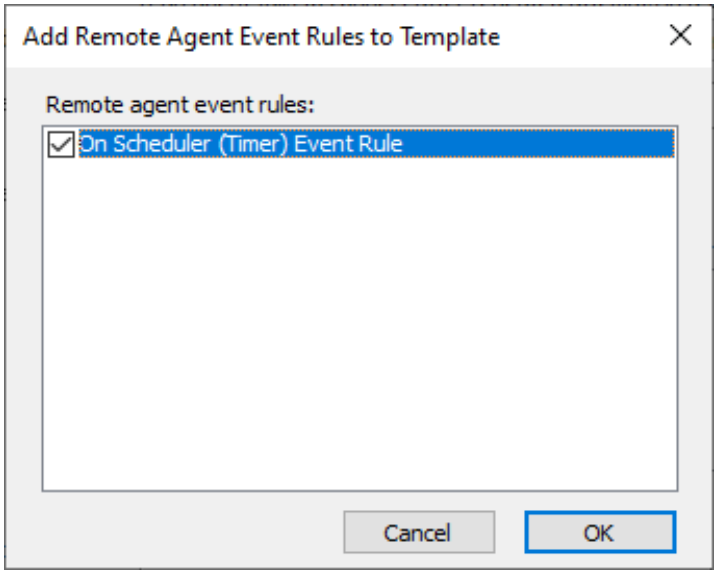


3. On the **Remote Agents**tab, click **Add**. The **Remote Agent Template** dialog box appears.



- **Template name**- The default name is Template with a number after it (which is incremented for duplicate names). If you expect to have only one template, the default name is probably fine. However, if you anticipate having more than one, you should give the templates descriptive names, such as "Western Region," "Los Angeles office," or "District 7." (Up to 130 characters.)
- **EFT host address**- Not editable in this dialog box
- **Update interval**- Specify when to contact EFT to check for and download updates. (Hourly, Daily anytime, Daily after-hours, Weekly, Weekly on weekends, Monthly)
- **Update failure** - Specify the action to take if an agent fails to connect after repeated attempts in 24 hours. Options are: Stop and disable the agent service and unenroll the agent, Stop and disable the agent service, or Stop the agent service only (do not disable it).
- **EFT home folder assignment**- Agent's home folder in EFT
- **IP access/ban list** - Opens the **IP Access Rules** dialog box to view, add, edit, or remove IP addresses that are denied or allowed access to the Site.

- **Rules**- Click the PLUS SIGN to add Event Rules to this template. The **Add Remote Agent Event Rules to Template** dialog box appears. [Disabled rules will show as (Disabled)]



  - Click a Remote Agent Event Rule, then click **OK**.
- **Agent install URL** - The default path to install the EFTRemoteAgentBundle.exe appears in the box. By default, the script reads:

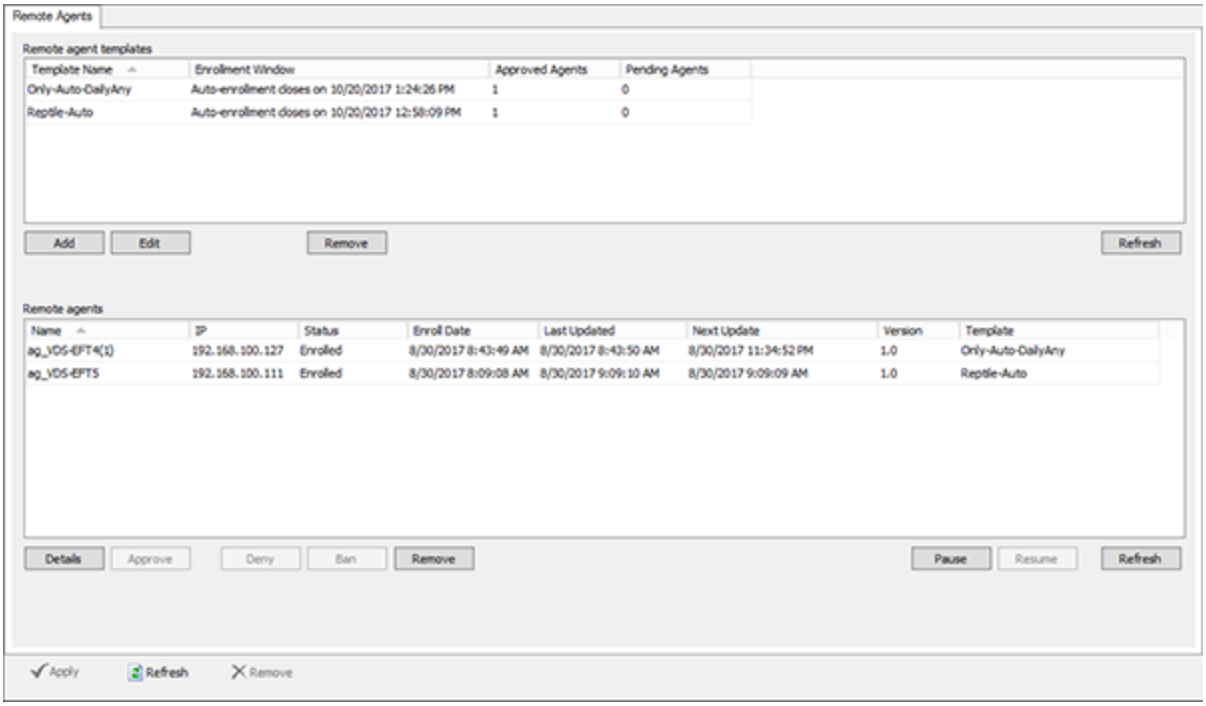
```
EFTRemoteAgentBundle.exe /i acceptEula="yes"
host="localhost" port=443
tid="5d93bdfb-40a6-4f7e-b5da-8a67ac0d53f7"
```

  Click **Script** to view the details. You should edit this to change the host and port number if you're not using "localhost" and port 443. (Port can be changed on the Site > Connections tab)

- **Agent Template ID** - The ID (tid) assigned to this template (read-only)
- **Agent enrollment**- Specify whether Remote Agents are manually or automatically enrolled:
  - **Auto enrollment**- If the Agent tries to install outside of the auto-enrollment windows the Agent will disable. A new template will have to be created and the Agent will have new template parameters. If **Auto-enroll** is chosen, the default expiration is 2 weeks from creation date.

- **Manual enrollment**- If the Agent is approved on the EFT side but the Agent doesn't answer for 6 days due to network connection, turned off, and so on., the service stops but stays enabled so that the next time the machine has connectivity it can enroll. ("Enrollment failure" appears in the **Status**column.)

4. Click **OK** to save the template. The template appears in the **Remote Agents** tab.



On the **Remote agents** tab, the following details are displayed:

- Template name - Displays the name of the Remote Agent template
- **Enrollment Window**- For automatic enrollment, this column indicates when the enrollment opportunity expires. Otherwise, it displays **Manual enrollment**.
- **Approved Agents**- Displays the number of Remote Agents that are using this template.
- **Pending Agents** - Displays the number of Remote Agents that have requested enrollment.
- **Name** - Remote agent name
- **IP** - Remote agent IP address
- **Status** - Enrolled, awaiting enrollment, decommissioning
- **Enrolled date** - Date/time when Remote agent was enrolled
- **Last updated** - Date/time of last Remote agent update
- **Next update** - Date/time when agent is scheduled to check for updates
- **RAM version number**- Version of RAM
- **Template name** - Name given when you defined the template

Managing templates:

- **Add** - Click to create a new template
- **Edit** - Opens the Remote Agent Template dialog box so you can make changes. You cannot edit the following settings: host address, home folder assignment, and Agent enrollment period, (because doing so would cause the Remote Agent to fail).
- **Remove** - Deletes a selected template.
- **Refresh** - (top pane) Refreshes the list of approved and pending agents.

Setting changes that affect both new agents that enroll with this template as well as existing agents the next time they call home include:

- update interval
- agent rules assignments
- IP access/ban list

Settings that cannot be changed so as to not break deployed agents include:

- certificates
- host address

- home folder assignment
- agent enrollment period

Managing agents:

- **Approve**- Enables a Remote Agent that has requested enrollment
- **Ban** - Prevents the Remote Agent from requesting access
- **Deny** - Denies an enrollment or updates request
- **Details -**Refer to Managing Remote Agents.
- **Pause**- Pauses the Remote Agent Event Rules. The Remote Agent will still check for periodic updates on its defined update schedule.
- **Refresh** (bottom pane) - Refresh the list of agents to see updated status
- **Remove** - (bottom pane) Deletes the selected Remote Agent. Also know as decommissioning.
- **Resume**- Resumes the Remote Agent Event Rules to run at the next update interval.

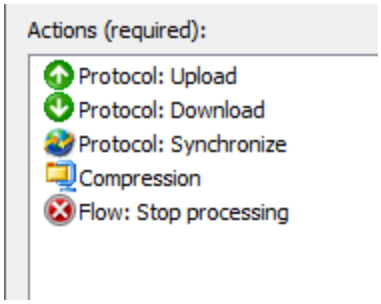
Refer to Managing Remote Agentsfor details of managing Remote Agents.

Remote Agent Rules

The **Remote Agent Rules** tab is where you can define automation rules that apply to the Remote Agents. The Remote Agent Event Rules trigger on the Remote Agents that you assign the rule to, not on EFT.

The Remote Agent Rules have limited triggers and Actions available, separate from EFT Event Rules:

- Event triggers for Remote Agents include Schedule (Timer) events, and Folder Monitor and Folder Monitor Failed events.
- Event Actions for Remote Agents include Upload, Download, Synchronize, Compression, and Stop processing this rule action.



Enrolled agents "call home" periodically to obtain their automation instructions, configurable in the Remote Agent template. If connection or authentication fails, the agent will perform retries as specified in the Remote Agent Event Rule configuration. If all connections/retries fail, then the Remote Agent Event Rule fails.

- Agents receive their rules on their update interval.
- Paused rules will take effect when the agent updates according to its update interval.
- Resumed rules will take effect when the agent updates according to its update interval.
- Remote agent rules can be created before or after template creation.

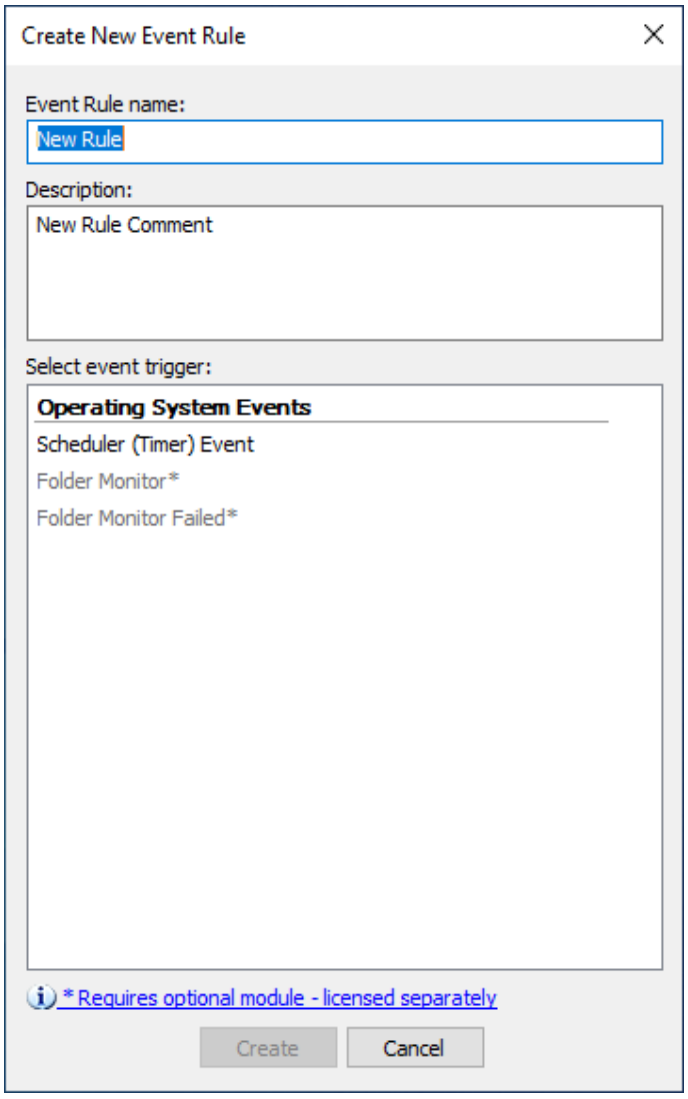
Automation instructions are configured within EFT Event Rules, allowing administrators to specify one or more “hot” folders the agent should monitor (relative to the agent’s file system), or a schedule, including complex recurring schedules, in which to initiate a transfer. Transfers can be uni- or bi-directional, meaning files can be uploaded from the agent or downloaded from EFT, depending on the desired outcome.

If an agent is properly enrolled, EFT will automatically authenticate the agent on connect, and authorize the agent to write to a designated home directory on the server. IT can optionally setup server-side Event Rules to then initiate automation sequences within EFT based on agents initiated transfers, thus completing the cycle of agent automation, agent transfer, central server receipt, and central server automation, such as integrating received files into a back-end system.

Keep in mind that their VFS folderis their home folder when defining Remote Agent Event Rules.

To create a Remote Agent Rule

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, expand the Site node, then click **Remote Agent Event Rules**.
3. Next to the **Rules**pane, click **New**. The **Create New Event Rul**e dialog box appears.



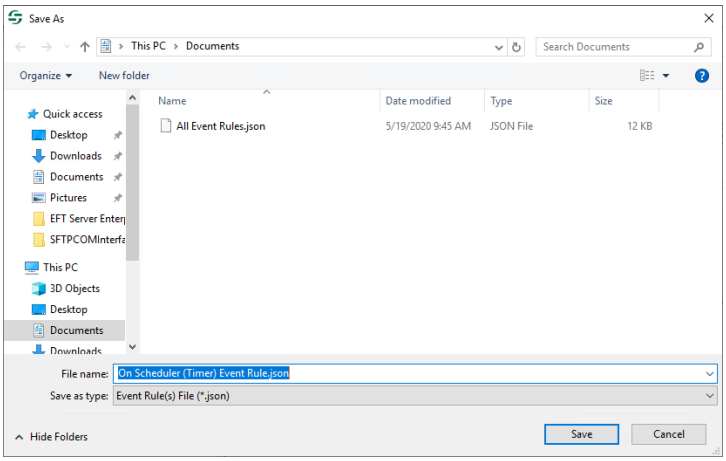
4. Click an event trigger: Scheduler (Timer) Event, Folder Monitor, and Folder Monitor Failed.
5. Finish defining the rule, then click Apply.

   The rule is now available for you to assign to Remote Agents in the Remote Agent template.

Exporting and Importing Remote Agent Rules

To export Remote Agent Rules

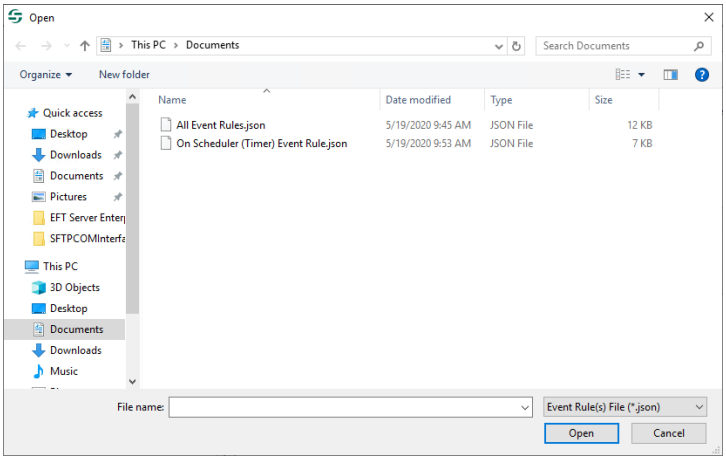
1. Right-click the Remote Agent Rule that you want to export, then click **Export Remote Agent**. The Windows **Save As** dialog box appears.



2. Click **Save**. The rule is saved as a JSON file with the name you gave it. A message appears to confirm that it was saved.
3. You can view and edit JSON files in a text editor, such as Notepad.

To import Remote Agent Rules

1. Right-click the rule that you want to import, then click **Import Remote Agent Rule(s)**. The Windows **Open** dialog box appears.



2. Click **Open**. The rule is added to the **Remote Agent Rules** node.

   A message appears to confirm that it was imported and you are offered the option to view the log. The log file is saved to the logged-in user's \Appdata\Local\Temp\EFT folder. The Remote Agent Rule GUID, the name of the rule, and success or failure of import appears in the log.

3. If an rule exists with the same name as the one being imported, a number is added to the name in the tree.

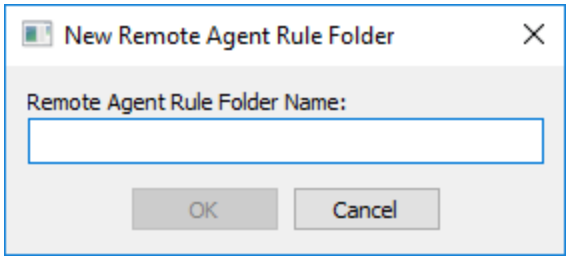
4. After the rule is imported, you can drag and drop it into an Remote Agent Rule Folder and edit it, just like any other rule.

Remote Agent Rule Folders

Remote Agent Rules can be organized into folders for easier management and organization. You can also apply permissions to an Remote Agent Rule folder that apply to all Remote Agent Rules in that folder. You can "drag and drop" Remote Agent Rules into a folder, and create new Event Rules within a folder. (You cannot create subfolders in folders.)

To create an Remote Agent Rule folder

1. Click the Remote Agent Rules node, then click **New Remote Agent Rule Folder**. The **New Remote Agent Rule Folder** dialog box appears.



2. Provide a name for the folder, then click **OK**.
3. Click **Apply**.
4. Now you can click and drag rules into your new folder and add permissions.

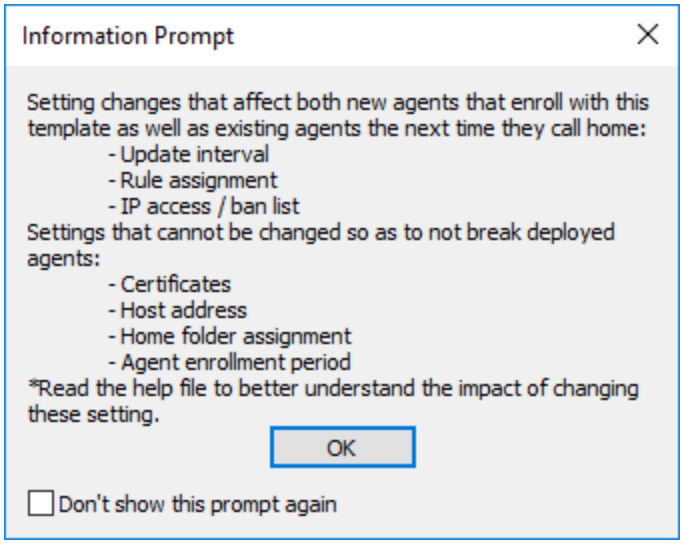
Remote Agent Context Variables

The Remote Agent Context Variables can be used in RAM Event Rules. Each of the variables is described below.

Text Displayed	Variable	Description
Remote Agent Name	%AGENT.NAME%	Computer name of remote system running the Remote Agent, enumerated if there is more than one Agent with that name.
Remote Agent Version	%AGENT.VERSION%	Version of Remote Agent update
Remote Agent Last Update Time Stamp	%AGENT.LAST_ UPDATE_TIMESTAMP%	Date of last Remote Agent update
Remote Agent Next Update Time Stamp	%AGENT.NEXT_ UPDATE_TIMESTAMP%	Date of next scheduled Remote Agent update
Remote Agent NetBIOS Name	%AGENT.COMPUTER_ NAME%	Computer name of remote system running the agent
Remote Agent Template	%AGENT.TEMPLATE%	Template name associated with the Agent
Remote Agent Status	%AGENT.STATUS%	Status of Remote Agent (e.g., Active, Pending, Approved, Denied, Banned)

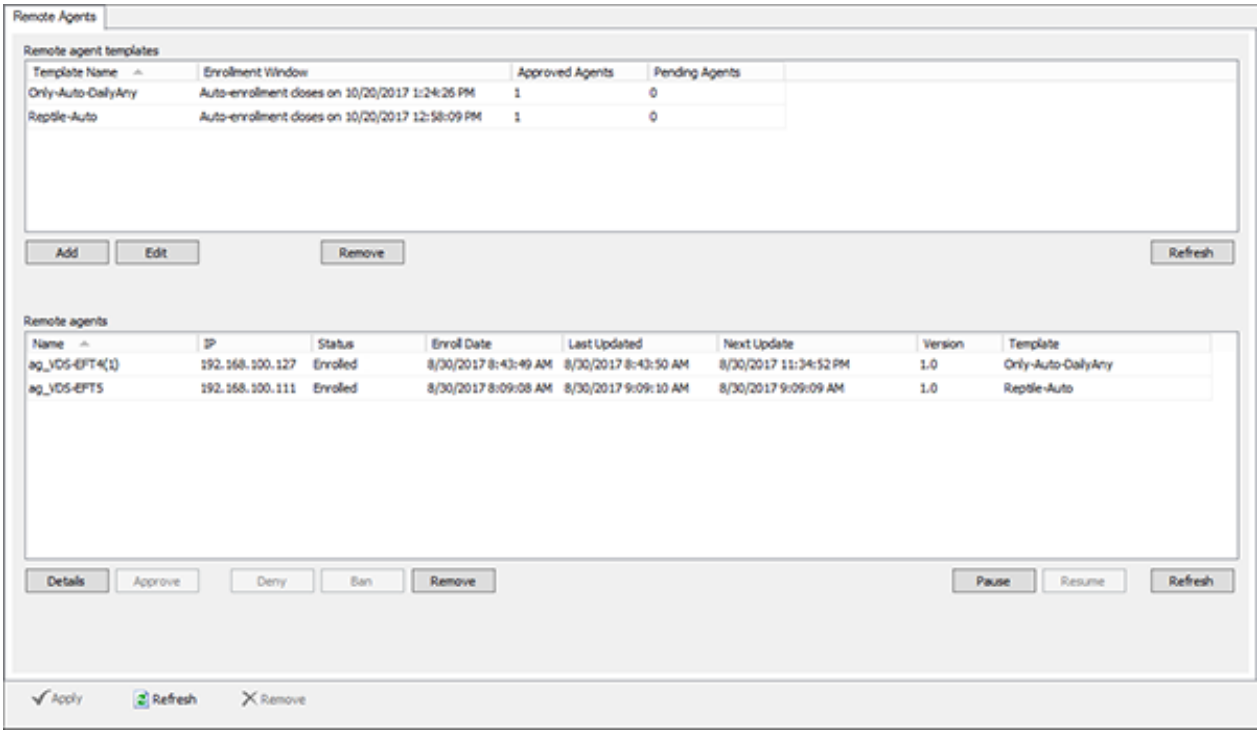
Managing Remote Agents

As Remote Agents request enrollment and updates, the Remote Agent's information appears in the bottom half of the **Remote Agents** tab of the Site.

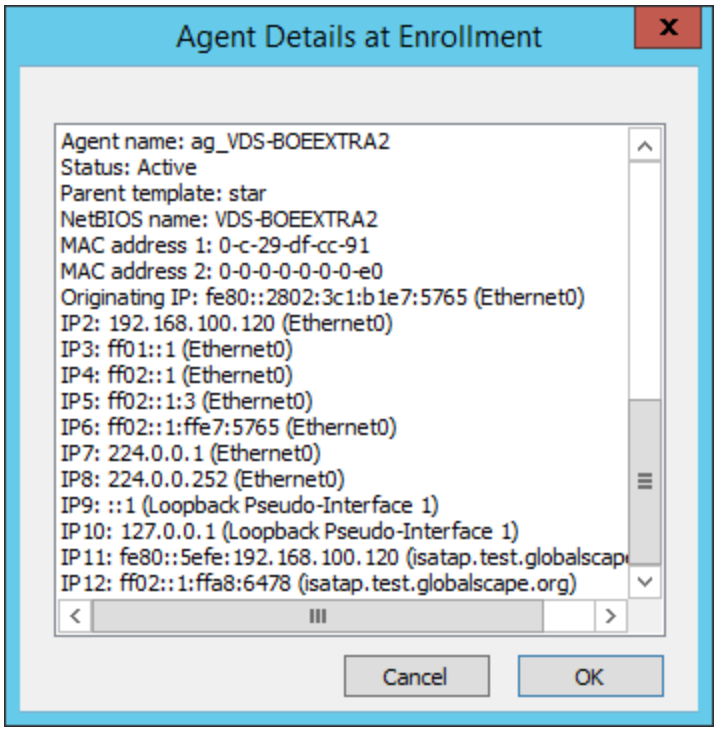


To manage Remote Agents

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, expand the **Site** node, then click **Remote Agents**.
3. In the bottom half of the **Remote Agents** tab, click the name of the Remote Agent that you want to manage.



- **Details** - Displays information about the Remote Agent: name, status, template, MAC addresses, IPs. Click **OK**to close the dialog box.



- **Approve** - Enables a Remote Agent that has requested enrollment
- **Deny** - Denies an enrollment or updates request
- **Ban** - Prevents the Remote Agent from requesting access

- **Remove**- Deletes the selected Remote Agent. Also know as decommissioning.
- **Pause**- Pauses the Remote Agent Event Rules. The Remote Agent will still check for periodic updates on its defined update schedule.
- **Resume**- Resumes the Remote Agent Event Rules to run at the next update interval.
- **Refresh**- Refreshes the list of approved and pending agents.
- **Export** - Exports the status of the selected Agent.

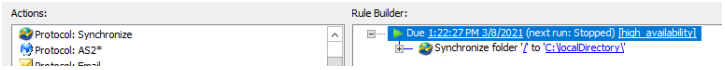
See also Remote Agent Templates.

Sending Files to a Different Server

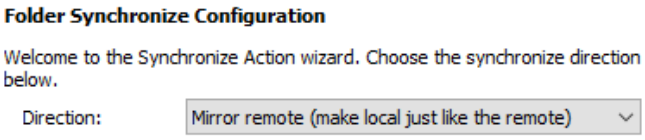
RAM Agents can send files (download/offload) to another server using RAM Event Rules. By default, all RAM Agents have an HTTPS connection to the EFT that manages that Agent. The EFT administrator can specify a different protocol, host, port, username, and password to allow the Agent to offload (send) files to another EFT or any other server to which you have credentials. Using a Download Action, in the Download Action Wizard, you can specify other protocols, including LAN copy using UNC paths on the local network.

To synchronize files across remote servers

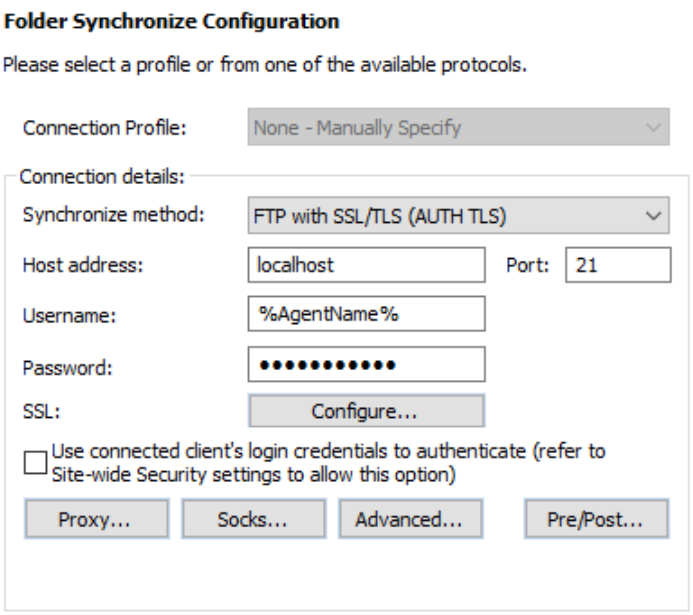
1. Configure a **Protocol: Synchronize** RAM rule



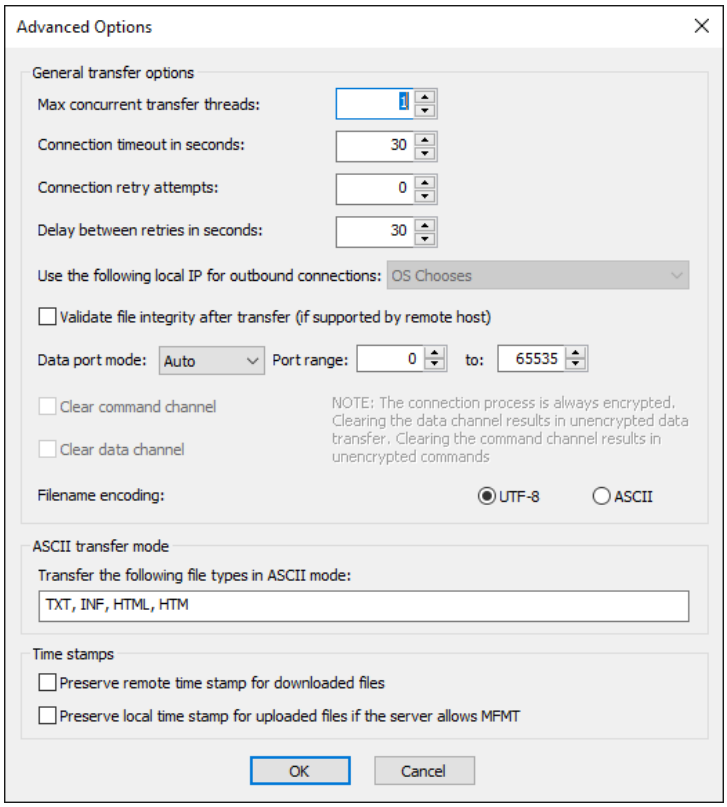
2. Set the rule to "Mirror remote":



3. If you have a critical need for the timestamp to match, use the FTPS protocol for RAM synchronization; otherwise, when synching files that are more than 6 months older, the date will be correct, but the timestamp will be off. (This is a limitation in the SFTP implementation in EFT at this time.)

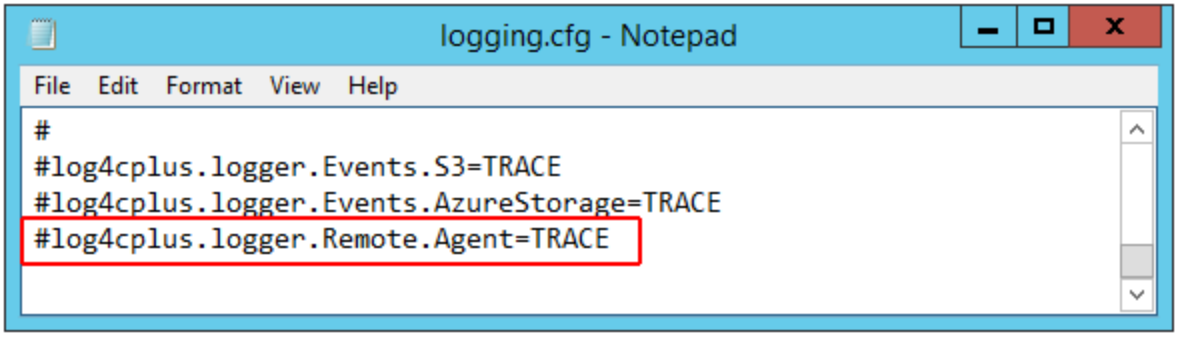


4. Set the **Advanced** option for **Preserve remote time stamp for downloaded files**.



Remote Agent Logging

On the EFT server, remote Agent events can be tracked in the EFT.log file on EFT. By default, the Remote Agent log is commented out in logging.cfg.



On the Remote Agent's computer, there is also a file named agent.log that contains updates, errors, event rules it has received, and so on.

To enable logging of Remote Agent events

1. On the EFT server computer, open **C:\ProgramData\Globalscape\EFT Server\logging. cfg** in a text editor.
2. Scroll to the very bottom, to

   `#log4cplus.logger.Remote.Agent=TRACE and remove the POUND SIGN #`

   TRACE level should be sufficient.

The EFT.log file entries will look something like this:

```
09-07-17 17:07:24,071 [2520] INFO Remote.Agent <>
 - Template Template (1) added by administrator
 09-07-17 17:14:59,634 [2520] INFO Remote.Agent <>
 - Template Template (2) added by administrator
 09-12-17 16:02:39,094 [2524] INFO Remote.Agent
<HTTP.ProcessRequest>
 - Processing agent initial enrollment request.
09-12-17 16:02:39,203 [2524] INFO Remote.Agent
<HTTP.ProcessRequest>
 - Agent ag_NUCQT7MG9OH auto-enrolled.
```

Remote Agent activity also appears in the server log file, e.g., **C:\ProgramData\Globalscape\EFT Server\Logs\u_ex170912.log**:

```
2017-09-12 21:02:39 192.168.64.141 - - [1]POST
/boe/v1/enrollments
 - 200 345 813 - 443
 2017-09-12 21:02:39 192.168.64.141 - - [2]POST
/boe/v1/enrollments/6d01ab2a-f523-4eb1-8b53-d8c608b128b0
 - 200 6178 292 - 443
2017-09-12 21:02:39 192.168.64.141 - - [3]POST
/boe/v1/agents/6d01ab2a-f523-4eb1-8b53-d8c608b128b0
 - 401 313 216 - 443
 2017-09-12 21:02:39 192.168.64.141 - ag_NUCQT7MG9OH [4]user
 ag_NUCQT7MG9OH - 331 - - - 443
2017-09-12 21:02:39 192.168.64.141 - ag_NUCQT7MG9OH [4]pass
 ****** - 200 - - - 443
2017-09-12 21:02:39 192.168.64.141 - ag_NUCQT7MG9OH [4]POST
 /boe/v1/agents/6d01ab2a-f523-4eb1-8b53-d8c608b128b0 - 200 3230
299 - 443
2017-09-12 21:02:39 192.168.64.141 - - [5]POST
/boe/v1/agents/6d01ab2a-f523-4eb1-8b53-d8c608b128b0
 - 401 313 216 - 443
2017-09-12 21:02:40 192.168.64.141 - ag_NUCQT7MG9OH [6]user
 ag_NUCQT7MG9OH - 331 - - - 443
2017-09-12 21:02:40 192.168.64.141 - ag_NUCQT7MG9OH [6]pass
 ****** - 200 - - - 443
2017-09-12 21:02:40 192.168.64.141 - ag_NUCQT7MG9OH [6]POST
 /boe/v1/agents/6d01ab2a-f523-4eb1-8b53-d8c608b128b0 - 200 3230
308 - 443
```

The Remote Agent computer also has logs in **C:\ProgramData\Globalscape\EFT Remote Agent**. Trace-level logging must be enabled in agentlogging.cfg. An administrator can remote access the RAM computer and use a utility such as Baretail to actively monitor what the agent is doing.

```
C:\ProgramData\Globalscape\EFT Remote Agent\Agent.log
```

```
C:\ProgramData\Globalscape\EFT Remote Agent\agentlogging.cfg
```

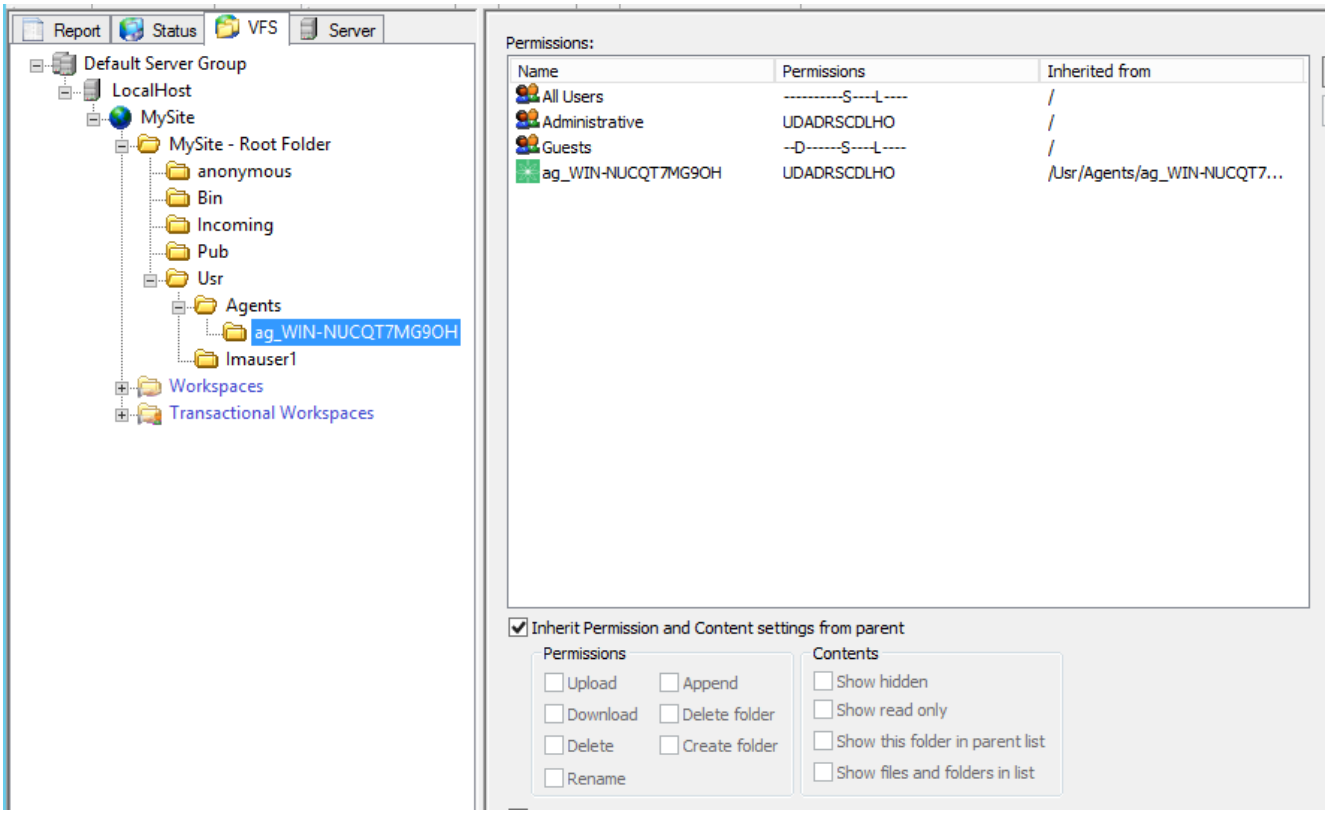
More logging on specific transfers in the following directory (similar to how EFT does it by default):

```
C:\ProgramData\Globalscape\EFT Remote Agent\logs\
```

Remote Agents in the VFS

After a Remote Agent connects, a home folder for that Agent is created in the VFS. The Remote Agents will each have their own /Usr/ folder in the VFS system. This is important to understand when creating Remote Agent Event Rules.

Each Remote Agent has its own home folder and has every permission so that it can upload, download, create folder, delete files and folders (in its own home folder), rename, and append files. EFT administrators can add/remove permissions via VFS; however, they cannot remove an agent in the VFS.



Related Topics

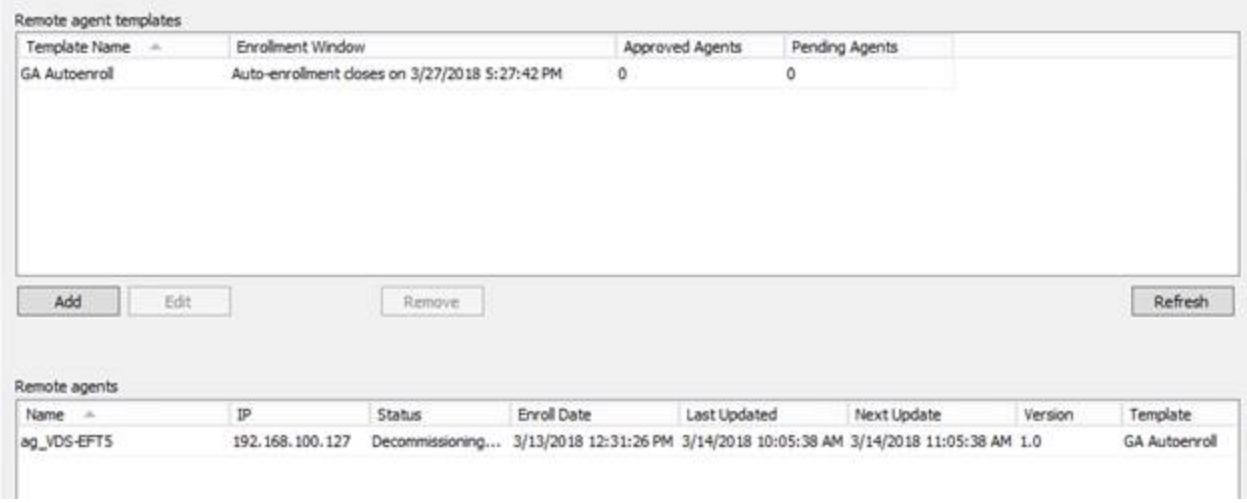
- Specifying Permissions to Folders (VFS)

Decommissioning a Remote Agent

If you need to remove a Remote Agent so that it no longer connects to EFT, you can decommission it. For example, when upgrading EFT, you must decommission any Remote Agents before upgrading them.

To decommission a Remote Agent

- In the **Remote agents** pane, click the Remote agent that you want to decommission, then click **Remove**. When the Remote agent checks in for updates, it will decommission itself.



Web Transfer Client and Workspaces

The topis below describe configuring and using the Web Transfer Client (WTC) and Workspaces with EFT.

- How Do I Share Files?
- WTC and Workspaces User Guide
- WTC and Workspaces Administration

How Do I Share Files?

Any user from anywhere in the world who has a computer with Internet browser or FTP client can access EFT and share files—provided the computer on which the user is attempting to connect to EFT is allowed access, and the user has an accountdefined on EFT. The user account itself or the group to which it belongs must have the appropriate permissions (upload, download, create folders, and so on) assigned on the VFS tab of the administration interface. When users log in to EFT, they connect only to their home folders and cannot browse above their home folders.

EFT allows the following methods through which you can share files using EFT:

- **Web Transfer Client (WTC)** - The WTC is EFT's browser-based file transfer client that allows users to transfer files over HTTP or HTTPS. The WTC can resume transfers and can send multiple files concurrently. It also has drag-and-drop support, integrity validation, a transfer queue, and no file-size limit. The number of files a directory listing can contain, the characters a file/folder name can contain, and the path length of directories is limited by Windows conventions. Refer to File-Naming Conventionsfor details. For regarding file-naming conventions, refer to the *Microsoft Windows Developer Network* article *Naming a File**and the Microsoft TechNet*article How NTFS Works.
- **Workspaces**- Users can create shared folders in which to share files with other EFT users through the Web Transfer Client. Additionally, if the EFT administrator allows it, you can share files with external users and share your Workspaces folders.
- **EFT Outlook Add-In** - With the EFT Outlook Add-In, users can send files via email and the recipient can pick them up in their web browser through Workspaces. Refer to Using EFT Outlook Add-In for details.
- **Mobile Transfer Client** (MTC) - The MTC is a mobile app that provides a way for iOS and Android phone and tablet users to securely connect to EFT and upload and download files while providing a number of centrally managed security controls for safeguarding your corporate data. Refer to Mobile Transfer Client (MTC) for details.
- **Globalscape's CuteFTP®** or a similar "FTP client" - Any FTP client can be used to connect to EFT and transfer files. For more information about CuteFTP, refer to https://www.globalscape.com/cuteftpor online help.
- **Windows File Explorer**- (Not available in EFT Arcus) When logged in to the EFT computer, administrators can manage files on EFT using Windows File Explorer. By default, user files are stored in the **C:\Inetpub\EFTRoot**folder in the **Usr** folder under the Site on which their account is defined (or, on HA

implementations, in the shared configuration path, e.g., **\\x.x.x.x\inetpub\EFTRoot\mySite\Usr\username**). In the illustration below, user **imauser**, defined on **GSSite**, stores files in the **imauser** folder. Anyone with the proper permissions on the EFT computer can drag and drop, copy and paste, and create and delete files and folders, just like in Windows File Explorer.

- **Command Prompt**- At a command prompt, you can enable an FTP session and transfer files, if you are familiar with basic DOS commands. Refer to the KB article "Can I use a Windows Command Prompt to send FTP commands to a server?" for list of common commands.

Related Topics

- Login In to EFT (WTC)
- Viewing Transfers To and From the Site
- Sending Files with the Outlook Add-In
- Emailing Files from within the WTC
- Sharing Folders (Creating a Workspace)

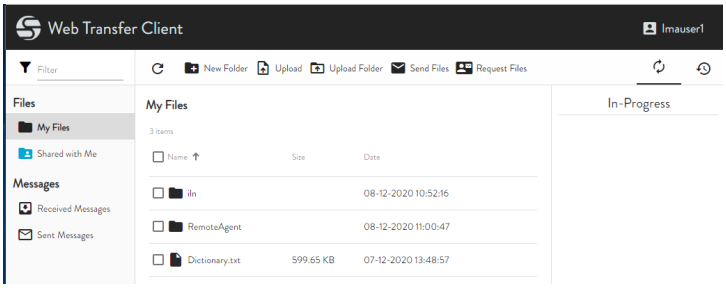
WTC and Workspaces User Guide

The procedures for configuring and using the Web Transfer Client are described in the topics below.

- Overview of the Web Transfer Client
- Logging In
- Personal Data and Privacy Settings
- Changing Your Password
- Sharing Folders (Creating a Workspace)
- Stop Sharing a Workspace
- Add Workspace Participants
- Edit-Remove Workspace Permission
- Register a New Account
- Downloading Files
- Uploading Files and Folders
- Resuming Transfers
- Canceling a Transfer
- Workspace and File Expiration
- Creating Folders
- Deleting a Folder or File
- Profile
- Drop Off Files
- Logging Out
- Pick Up Files
- Reply Page
- Request Files
- Send/Email Files in Workspaces
- Viewing Sent Messages
- Viewing Received Messages
- View Workspaces History
- Edit Notification Options
- Messages
- Notifications
- Workspace Comments
- File-Naming Conventions
- Filtering and Sorting the File List
- Moving Files between Folders
- Renaming a File or a Folder
- Searching for Files
- WTC Language Settings
- Web Transfer Client Pagination

Overview of the Web Transfer Client

The *Web Transfer Client* (WTC) is a browser-based file transfer client that allows you to transfer files over HTTPS to and from the EFT server. Using the WTC, you can upload and download files, pause and resume a transfer, cancel a transfer, move files between folders, create, rename, and delete folders and files, and share folders with other users. The WTC is also used as the interface for Workspaces.



Under **My Files**, you will see a count of the number of files and folders displayed. If you select one or more files and/or folders, it will display the number of items selected.

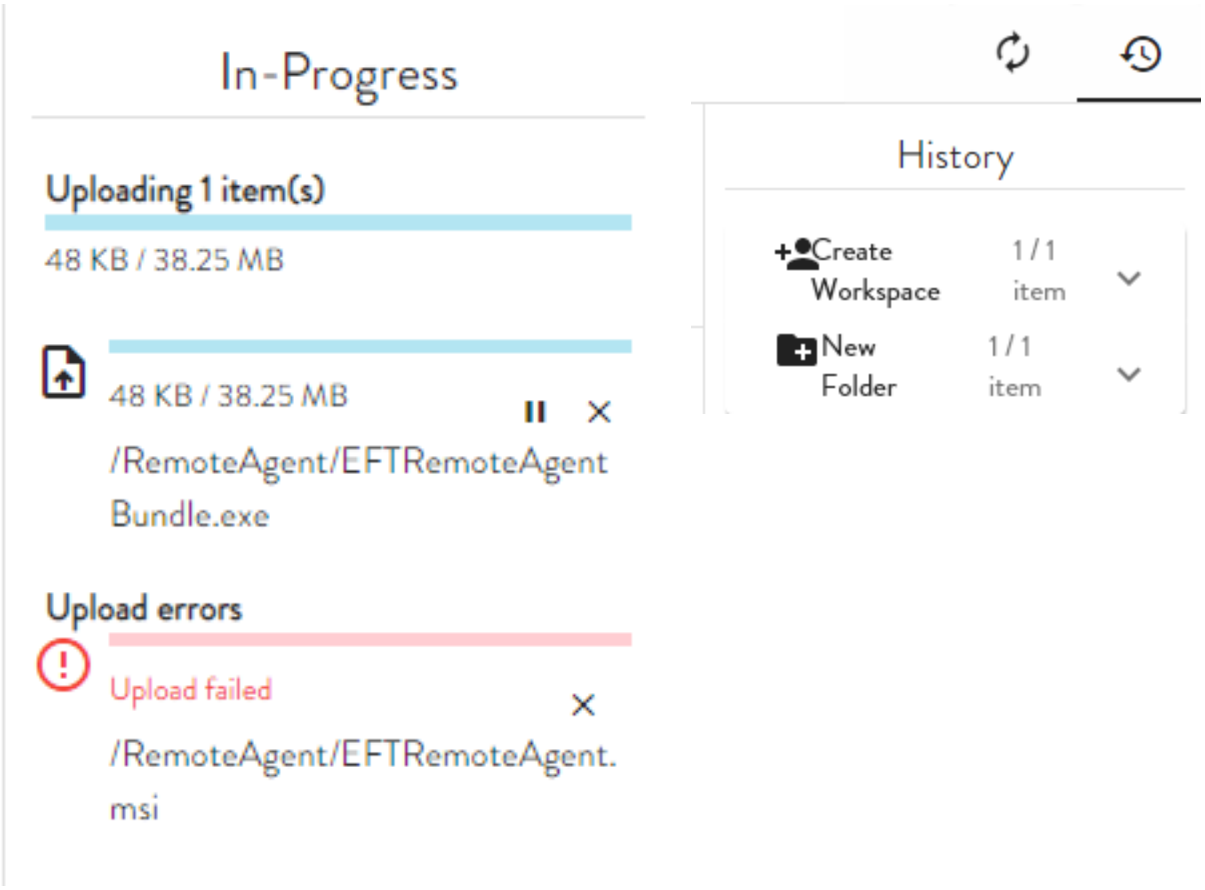
Toolbar

The toolbar icons that appear depend on what you have selected:

- New Folder, Upload, Upload Folder, Send Files, and Request Files appear when no files are selected.
- Share, Download, Rename, Move, and Delete appear when a file or folder is selected.

In-Progress and History Panel

Click the **In-Progress** icon to see files that are uploading or the **History** icon to view activities that occurred in the current session.



Some of the pop-up dialog boxes or messages in the WTC do not have a **Cancel** button or an **X**in the corner. To close those dialog boxes, click anywhere outside of that window and it will close.

For information about the Terms of Service and Privacy Policy, refer to Logging In.

Related topics:

- Logging In to the WTC
- Logging Out of the WTC
- Uploading Files and Folders
- Downloading Files
- Canceling a Transfer
- Resuming Transfers

- Filtering and Sorting the File List
- Searching for Files
- Error Messages and File Names
- Creating Folders
- Moving Files Between Folders
- Sharing Folders
- File Comments
- Renaming a File or a Folder
- Deleting a Folder or File
- Changing Your Password

Logging In

You can log in to the WTC and Workspaces in any supported browser. The system administrator will provide you with the URL (web address) and your login information.

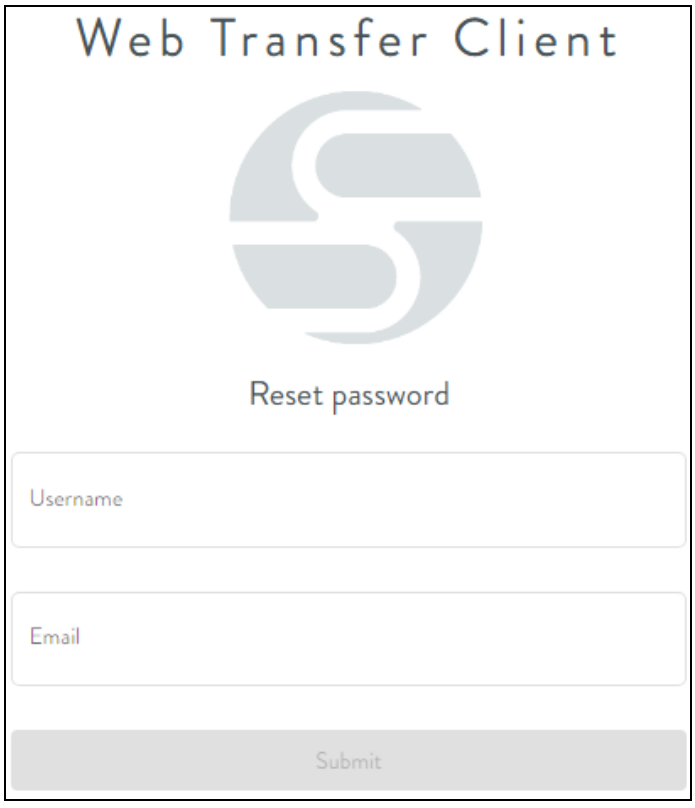
The EFT administrator should inform end users which IP address, port, username, and password should be used to log in to a Site. Because many users are unfamiliar with <IP address:Port> formatting, be sure to provide users with the exact URL that they should access to log in, whether they are accessing a Site from the Web Transfer Client, "plain-text" client, a command line, CuteFTP, or any other FTP client. For example, you could provide the link in an email.

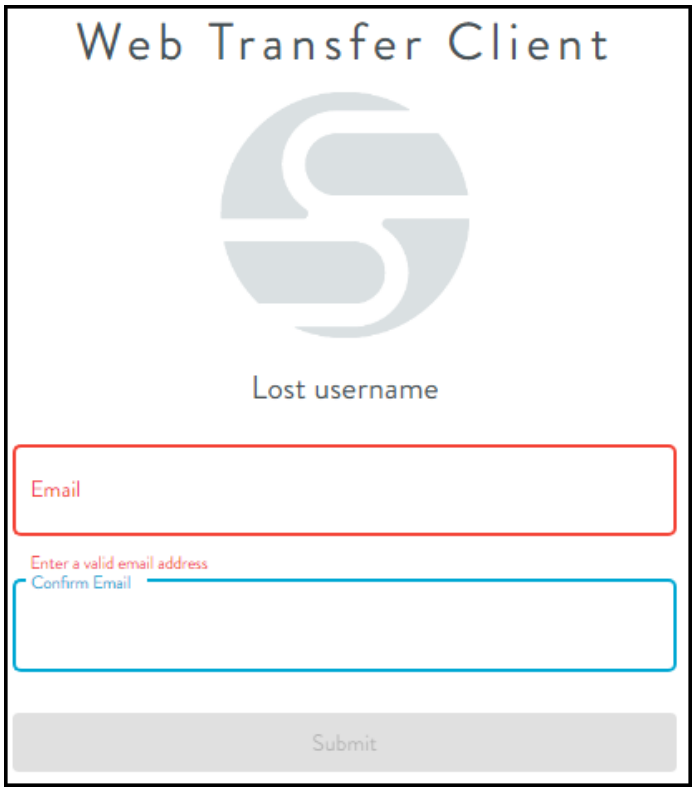
To log in

1. Open the web browser.
2. Type or click the web address provided to you by your system administrator. For example, type `https://www.ourfileserver.com`. The login page appears. (The **SSO Login** option appears if so configured.)

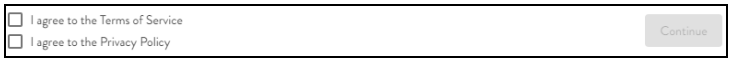
3. Provide your **Username**and **Password**, then click **Log In**. If you have been instructed to use secure sign-on, click **SSO Login**.

4. If you have been instructed to use two-factor authentication, you will be asked to provide a second response, such as a passcode. The EFT administrator can change the text that appears for the challenge. Refer to the article at https://kb.globalscape.com/KnowledgebaseArticle11267.aspxfor details.
5. If you don't know your username, click **Forgot Username** (if available). If you don't know your password, click **Forgot password**. In the dialog box that appears, provide your information and then click **Submit.**
    - If it is so configured in the EFT administration interface, users are prompted to change their password the first time they log in.
    - If a security prompt appears asking you to accept the website's certificate, select the **Always trust** check box, and then click **Yes**.
    - If a prompt appears to provide a passcode, use the method asked for in the prompt to retrieve your passcode (Email or SMS). In the dialog box that appears, provide your information and then click **Submit**. You will be asked for your email address to which the reset information will be sent. Your request is sent to the server and an automated response will email you your username.





- If you don't know your username, click **Forgot Username** (if available). Your request is sent to the server and an automated response will email you your username.
- If you don't know your password, click **Forgot password**.
- When the credentials are accepted by the server, the Web Transfer Client (WTC) appears.
- Depending on how the EFT administrator configured the WTC, you might see a box in which you can read and agree to the organization's Privacy Policy and Terms of Service.



- The administrator can configure EFT to require implicit or explicit agreement.
    - **Implicit** - Accept the agreement by using the WTC:
        - Click **Terms of Service** to read the agreement. Click anywhere outside of the agreement to close it.
        - Click **Privacy Policy** to read the policy. Click anywhere outside of the policy to close it.

    - Click the **X**to close the Terms of Service/ Privacy Policy box.
- **Explicit**- Select the **Agree**check boxes, and then click **Continue**.

Once you have accepted the agreement/ policy, your account information in EFT is updated to reflect your acceptance so that you don't have to accept the agreement/ policy every time you log in.

Related topic

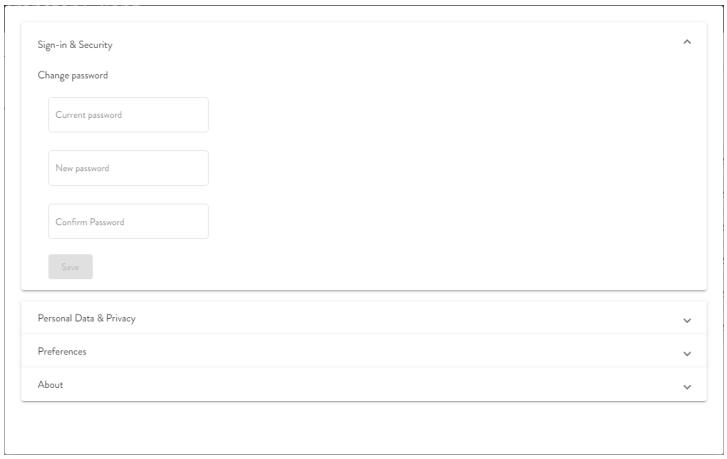
- Logging Out
- Terms of Service Agreement
- Privacy Policy
- SAML (Web SSO) Authentication

Changing Your Password

The administrator may have set your password to expire periodically. You can change your password within the Web Transfer Client. (The administrator must have enabled users to reset their passwords on the **Security** tab in the EFT administration interface.)

To change your password

1. In the upper-right corner, click your login name, then click **Profile**.
2. Click **Sign-in & Security**.



3. Provide your **Current password** and a **New Password**, and then **Confirm Password**. If the administrator requires complex passwords, a message will appear if your password does not meet the complex password or reuse password requirements.
4. Click **Save**. Click anywhere outside of the dialog box to close it.

Sharing Folders (Creating a Workspace)

You can invite internal and external users to share your folders, if the EFT administrator enables and configures Workspaces to do so. To share folders, the administrator has to have enabled Workspaces in the EFT administration interface on the **Web**tab of the Site. Workspace participants who were invited to share a Workspace cannot add participants to that folder, however, they can create new folders.

When the Workspace owner invites someone to join the workspace, EFT sends them the invitation via email. The invitation recipient clicks the link embedded in the email and then signs in to EFT (if an account has previously been created), or creates an account on EFT.

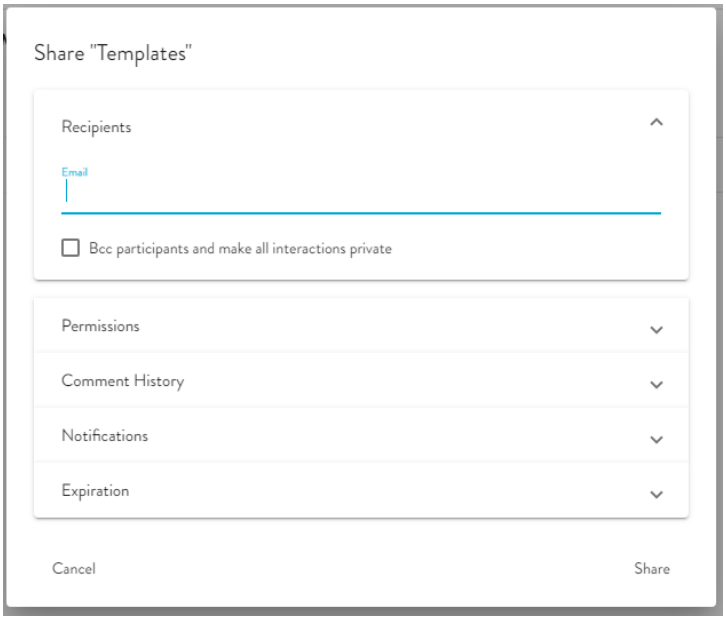
- Workspaces invitations expire after 5 days.

  If the Workspace invitation has expired before the invitee attempts to register, a prompt appears that says the invitation cannot be found.

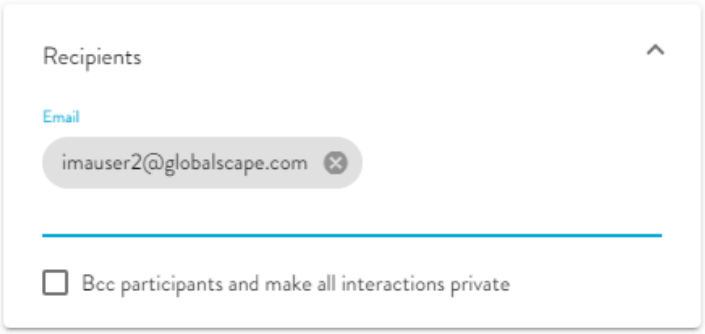
- Administrators can see and manage invited (guest) accounts in the administration interface on the VFS tab.

To share a folder

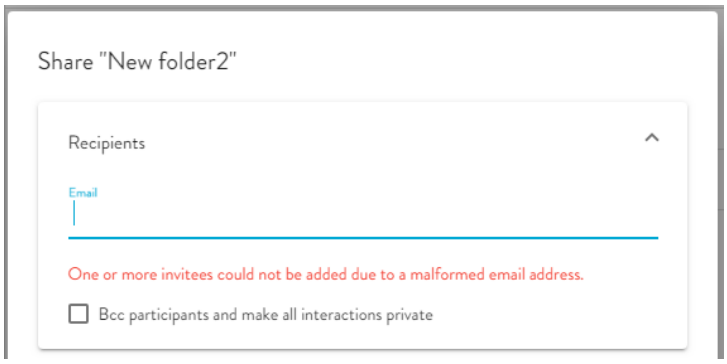
1. Log in to the Web Transfer Client.
2. Select the check box of the folder that you want to share, then click the **Share** icon. The **Share** dialog box appears.



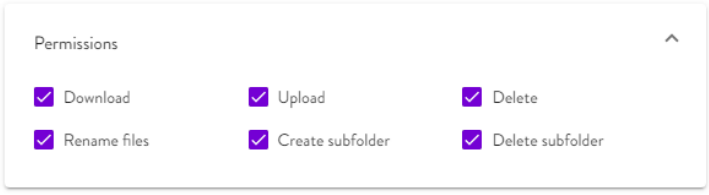
3. Provide email addresses of users with whom you want to share the folder. (You can later add or remove participants.) The email address appears in a gray box. (If it doesn't, press ENTER at the end of the email.)



   - If the email is not properly formed (username@domain.com) an error message appears.



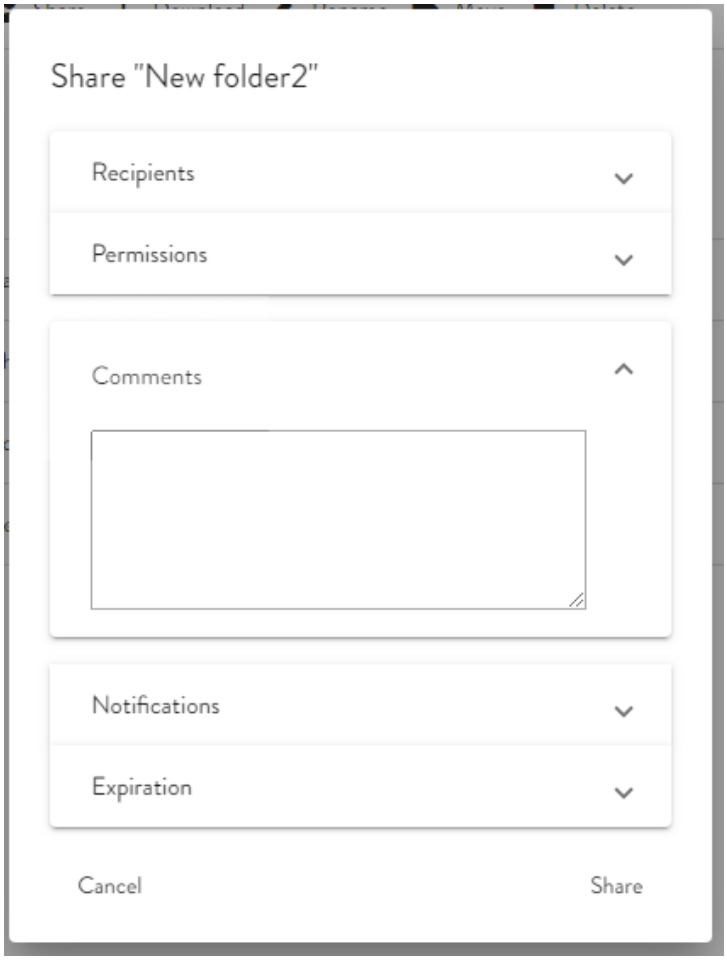
4. To create a private workspace, select the **BCC** check box. When a Workspace is private, the Alerts/Notification icon, the Workspace participants icon, and the comments icon are hidden from the recipient.
5. Assign permissions by clearing or selecting the check box next to that permission. By default, all permissions are selected (enabled). Clear the check boxes of the permissions that you do not want to assign to the users.



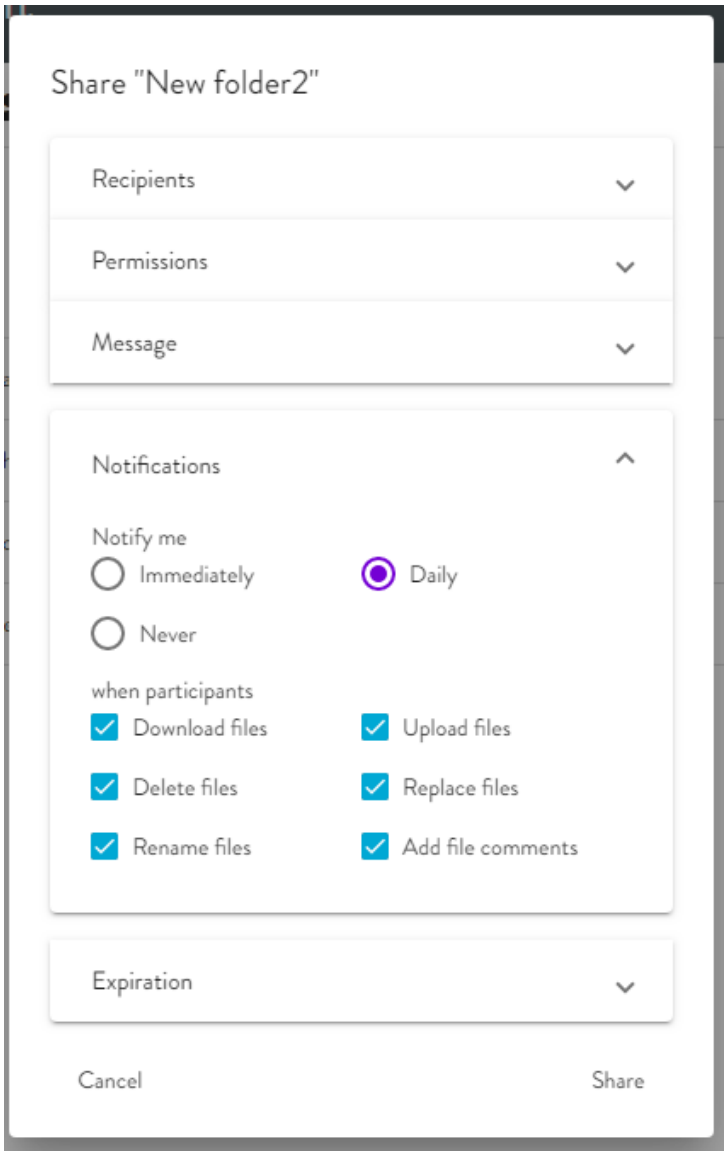
   The administrator can specify which permissions check boxes are selected by default, if any. The sharing user can still select the check box to enable the permission. Refer to Edit-Remove Workspace Permissionfor details.

Permissions that the administrator assigns to folders override any permissions that you assign. That is, if the folder that you are sharing does not have rename permission, you cannot assign that permission to the folder.

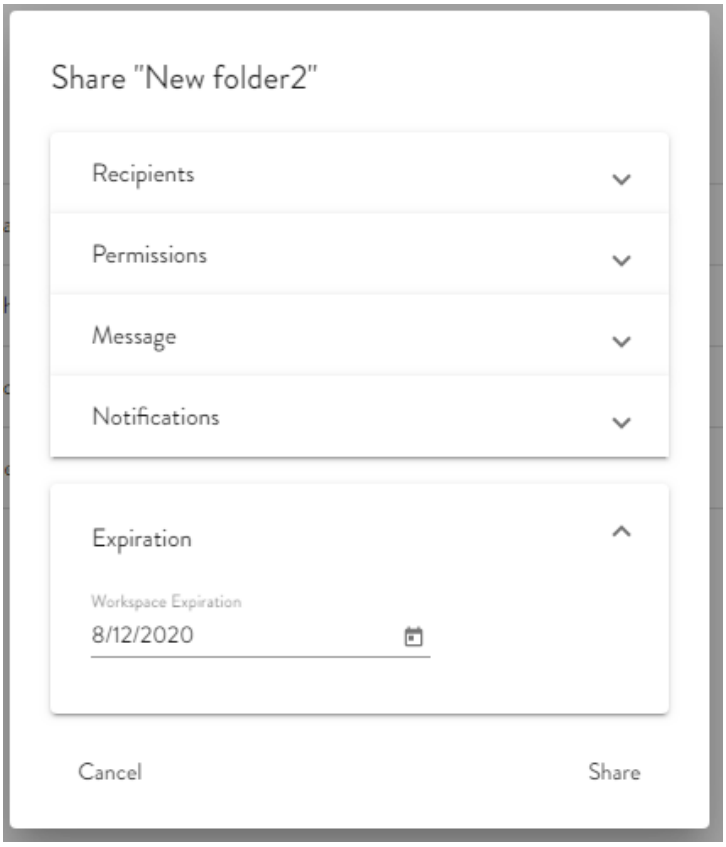
6. (Optional) In the **Comments** box, you can type comments. When you create a Workspace, the comment that you type in the **Comments** box appears in the invitation email.
    - View a history of comments added by clicking the shared folder and then clicking the comment icon.



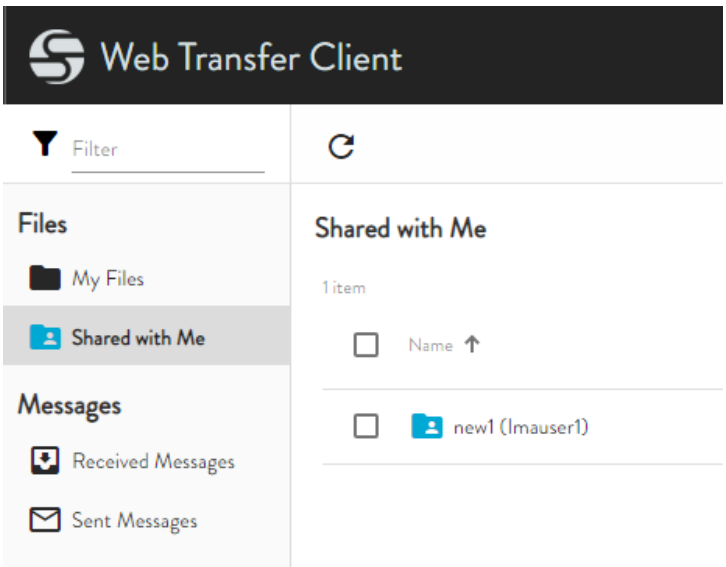
7. In the **Notifications**box, you can specify the type and frequency of email notifications about this Workspace.



8. (Optional) To expire the Workspace, click **Expiration**, and then specify the expiration date. The limit is specified in the administration interface in the **Workspaces - Share** dialog box on the **Site > Web** tab. (Alternatively, there is a Stop Sharing icon in the WTC toolbar.) The default expiration date appears, when defined in the administration interface.



9. Click **Share**. The Activity pane updates to indicate you've shared a folder. The users with whom you have shared the folder will see the shared folder in their **Shared with Me** tree. The username of the account that is sharing the Workspace appears in parentheses after the name of the folder (for example, *New Folder 2 (lmauser1)*).



Related Topics

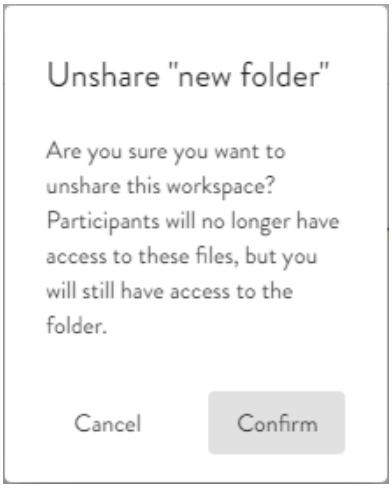
- Stop Sharing a Workspace
- Editing Workspaces Sharing
- Managing Workspaces in the VFS
- Transactional Workspaces
- Workspaces Invitations
- Workspaces Notifications

Stop Sharing a Workspace

When you no longer need to share a Workspace, you can "unshare" the folder.

To stop sharing the folder

1. Click the shared folder.
2. Click the **Unshare** icon. The **Unshare <folder_name>**message appears.



3. Click **Confirm**. Any user with whom you've shared the folder can no longer access the folder.

Related Topics

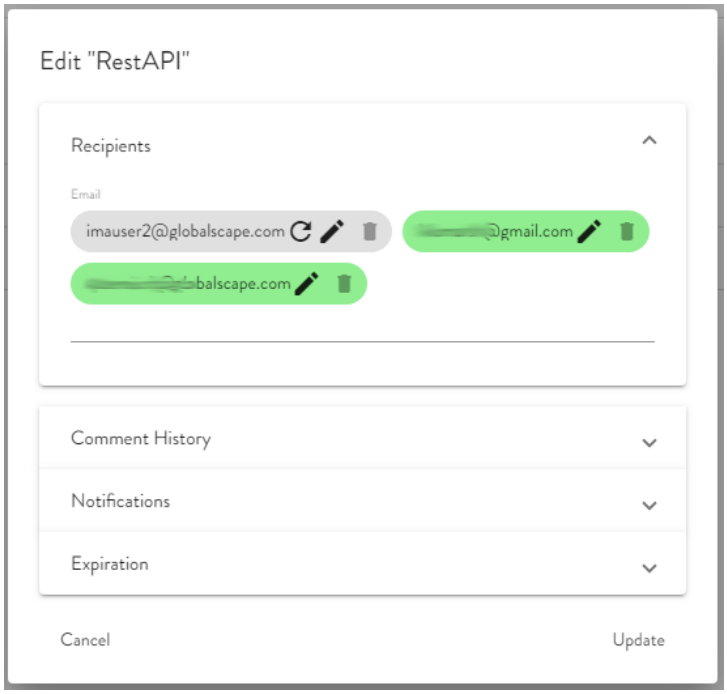
- Sharing Folders (Creating a Workspace)
- Managing Workspaces in the VFS

Add Workspace Participants

After you have created a Workspaceand invited participants to join the Workspace, you might later want to add participants.

To add participants

1. Click the check box next to the shared folder, then click the **Edit Workspace**.
2. Provide one or more additional email addresses, press ENTER. The box around the email address will turn green to indicate the user has been added to the Workspace.



3. Click the pencil icon to assign permissions, if different, then click **Update**.

Related Topics

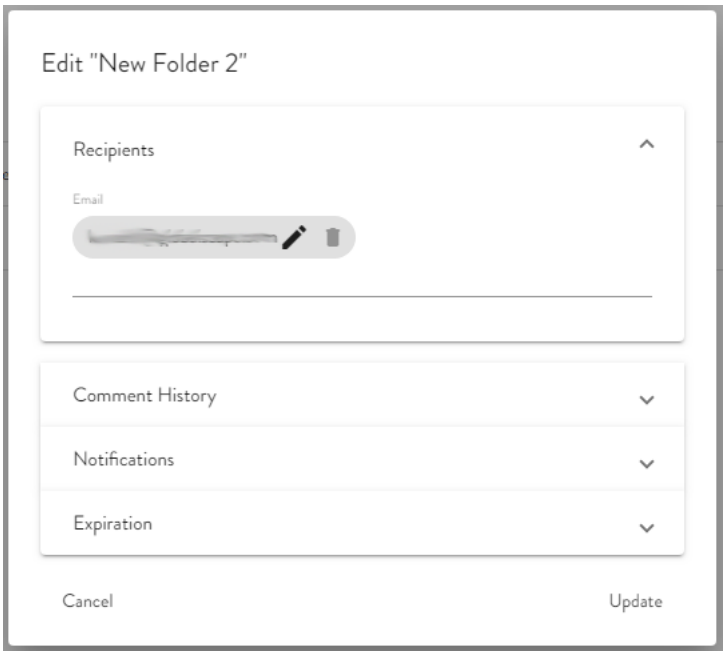
- Stop Sharing a Workspace
- Sharing Folders (Creating a Workspace)
- Expire a Workspace
- Edit Workspace Permission

Edit-Remove Workspace Permission

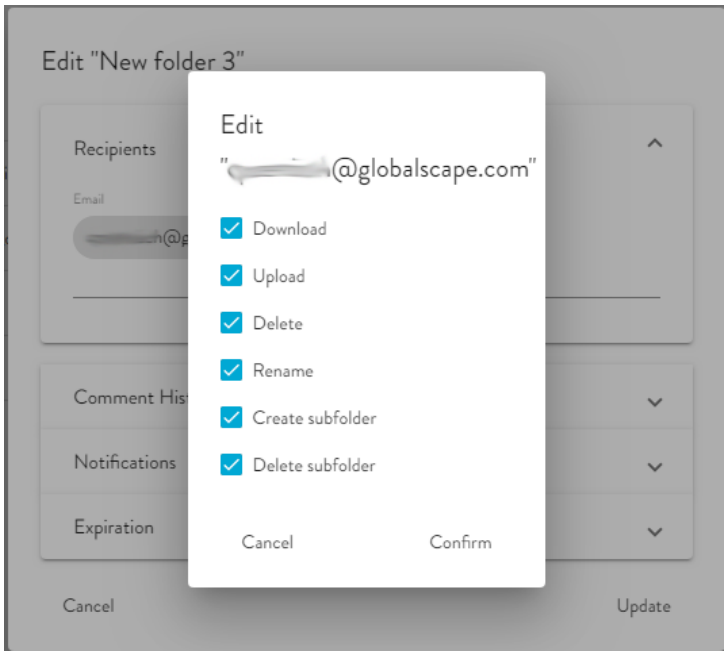
The default settings for Guest Users include **Download**, **Show this folder in parent list**, **Show files and folders in list**. Users with whom a Workspace is shared do NOT have permission to move files and folders out of the Workspace.

To edit a Workspace participant's permission or remove the user from the Workspace

1. On the tool bar, click the **Edit Workspace** icon.



- To delete the user, click the trash can icon.
- To edit the user's permissions, click the pencil icon for the user that you want to edit, then make the changes to the user's permissions, as needed.



2. Click **Update**.

Related Topics

- Expire a Workspace
- Add Workspace Participants

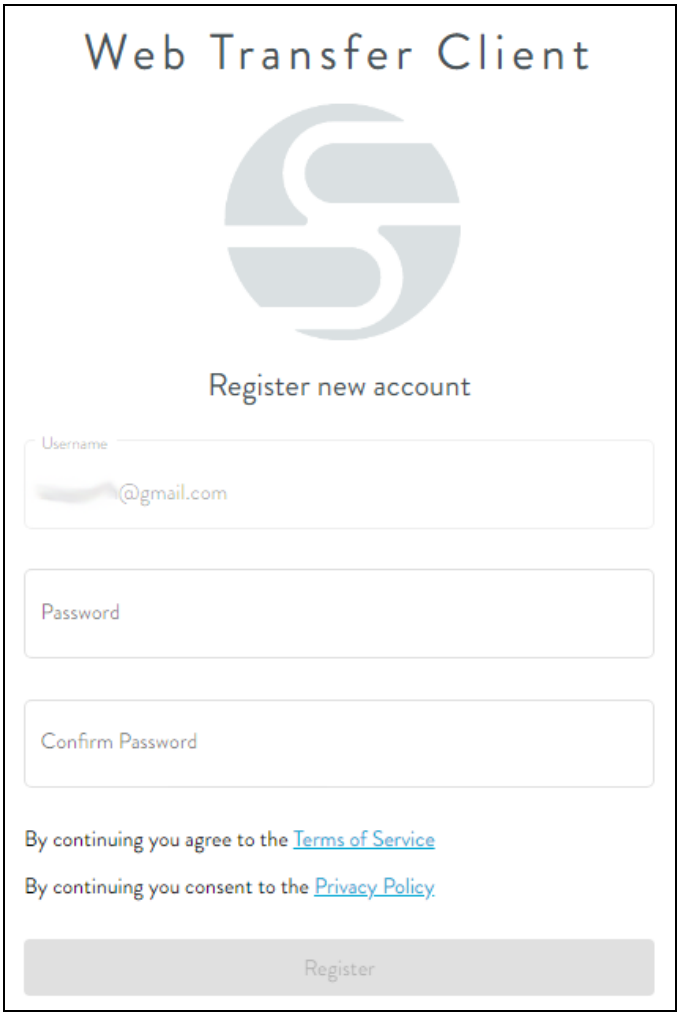
Register a New Account

When a Workspace creator invites others to a shared folder, an email is sent to each invitee.

If the Workspace invitation has expired before the invitee attempts to register, a prompt appears that says the invitation cannot be found.

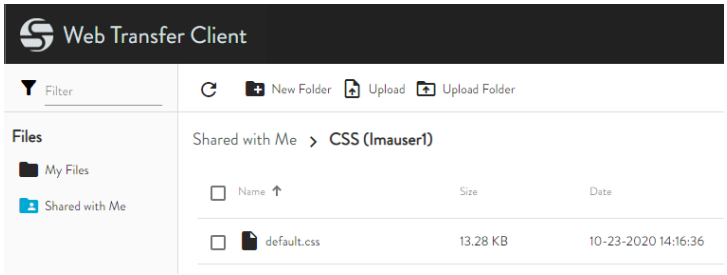
To join a Workspace

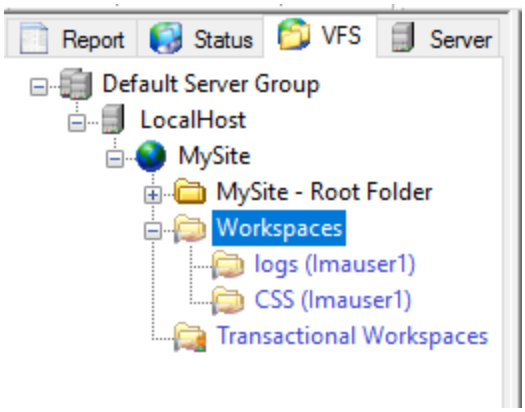
1. In the email invitation to join a Workspace (a shared folder), click **View Folder** (or right-click and then click **Copy link address**). The default browser opens with the WTC Registration page displayed.



2. The username for the account is the email address that the invitation is sent to. Create and confirm a password to register this username.

3. A one-time passcode is sent your email or or phone. Enter the passcode, then click **Submit**. The account verification process occurs, and then you can log in.
4. The Web Transfer Client appears and displays the folder that was shared with you. The username of the Workspace creator appears next to the shared folder and in the VFS in the EFT administration interface.





Downloading Files

You can download files from the server to your local computer on which you have download permission. The mechanism for downloading files is browser dependent. That is, Microsoft Edge/ Internet Explorer, Google Chrome, and Mozilla Firefox each has its own mechanism for downloading files.

- The Web Transfer Client does not support a CRC-check for downloaded files because of the limited access of the client file system. The process of initiating a download is human driven and is wholly managed by the browser itself, for security reasons. Further, the browser cannot arbitrarily read files on the local file system (for obvious security reasons), so EFT cannot read contents of downloaded files to do CRC32, and thus cannot issue a follow-up HEAD request to verify the integrity of the download.
- In certain browsers, if you are using a self-signed certificate you will receive a "network issue" warning when downloading files. Workarounds are to have a valid certificate, use special flags to ignore improper certificates, or not use HTTPS.
- The number of files per ZIP file download is specified in the WTC administrator JSON file (\EFT Server\Web\Shadowfax\wtc\assets\admin-configuration.json).

  ```
  "batchDownloadAsZipThreshold": 5
  ```

To download files

- Do one of the following:
  - **In the WTC**, click the file(s) you want to download, then click the **Download** icon. The file downloads to the folder defined in your browser's configuration. (To open your browser's **Downloads**folder, see below.) When you select multiple files or folders before clicking **Download**, they are downloaded as a ZIP file.
  - **In the Pickup Portal,** click one or more files that you want to download, then click the **Download** icon. The file downloads to the folder defined in your browser's configuration. (To open your browser's **Downloads**folder, see below.) When you select multiple files before clicking **Download**, they are downloaded as a ZIP file.
  - **For direct download In your browser**, copy and paste the URL provided by your administrator or in your company portal (for example, https://workspace.mycompany.com/directdownload/foo/MetaData2.db), then press ENTER. (This option is often referred to as "direct download" or "anonymous download.")

a. Login. The **Save As** dialog box appears and the file downloads.
b. Specify a location, if different, then click **Save**.

To open your browser's Downloads folder:

- In Chrome and Edge, click the **Settings**icon, then click **Downloads**(or press CTRL+J).
- In Firefox, click the green down-facing arrow to view most recent downloads, or type `about:downloads`in the address bar to view all downloads.
- In Safair, click the **Downloads** icon.

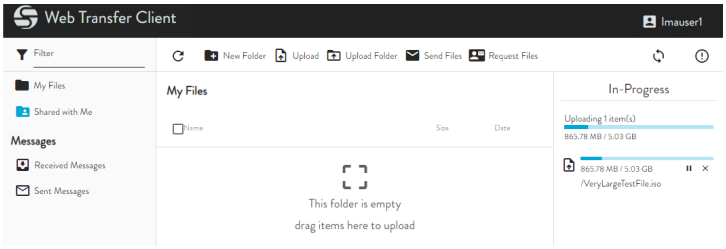
Uploading Files and Folders

In the Web Transfer Client, you can upload files and folders from your local computer to a remote server on which you have upload permission.

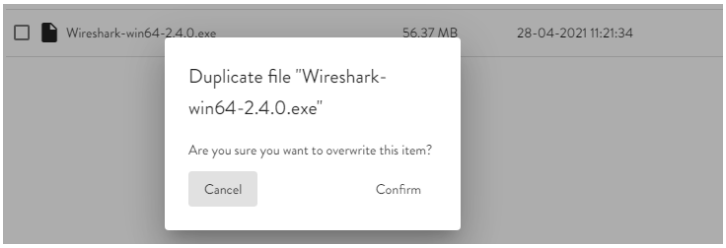
> **NOTE:** Web browsers are limited by available memory, CPU utilization, network performance, and numerous other factors. In the case of large files, you might want to compress (ZIP) it before you send it. Folder uploads and large file uploads are available in Chrome, Firefox, or Opera browsers only. If you want to upload folders in other browsers, you must compress them and upload the ZIP file. Because of the way EFT and Workspaces manage files, there are no limits on file size. However, EFT is at the mercy of the browser's capabilities and memory utilization, as well the capabilities of your computer.

To upload files between your local system and the server

- Do one of the following:
  - To transfer files and folders to the server, click **Upload**.
  - Click and drag one or more files or folders from your local file system to the file list. (Empty folders will be ignored and not transferred.)



- The PAUSE icon allows you to pause an in-progress transfer. If you want to clear the pane, you can click the CANCEL icon for each transfer
- When the file is transferred, if there is a file with a duplicate name already in your folder on the server, you are presented with a prompt asking if you want to overwrite the existing.



- You can upload multiple selected files at once by dragging and dropping from your local system to the WTC, or by clicking **Upload** and then selecting multiple files. The **In-Progress**pane displays the number of files selected to be uploaded until they are all uploaded. That is, if you are uploading 5 files and 3 of them have completed uploading, the display still says "Uploading 5 item(s)."
- If you have exceeded your allowed disk quota on the server, a message appears when you attempt to upload more files. To continue to upload files, you must delete some of your old files from the server or ask your administrator to increase your allowed disk quota.
- Before you can access the server using the WTC, the administrator must configure the server to allow WTC connections with your account.
- If network connectivity is lost while the WTC is transferring files, you can retry transfers that previously failed or were incomplete. If a file partially transferred before the connection went down, the transfer will be resumed from the point that it left off.

Resuming Transfers

A file transfer can be interrupted for various reasons, such as a network glitch, or you might pause the transfer yourself. When a transfer is interrupted because of errors, it will resume automatically after network connection is reestablished (up to 10 retry attempts over a 5-minute period).

To resume a paused transfer

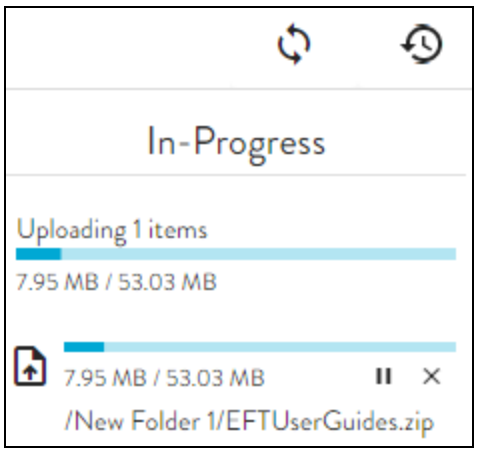
1. Transfers that have been interrupted appear in the **In-Progress** queue.
2. Next to the paused file, click the **Play**icon. The transfer will resume where it left off.

Canceling a Transfer

Most files that you transfer will transfer so quickly, you won't even notice. Larger files, however, will show progress in the **In-Progress**pane You can cancel an in-progress transfer.

To cancel a transfer

1. In the **In-Process**pane, while the transfer is in progress, click the PAUSE ⏸ icon.

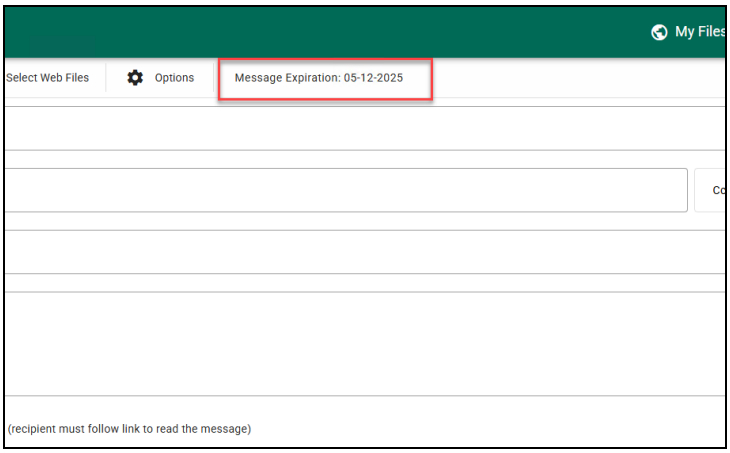


2. Click the PLAY ▶ icon to continue the transfer.
3. Click the **X** to cancel the transfer.
4. The pane is cleared after the transfer is complete.
5. You can show or hide the **In-Progress**pane using the circular arrows icon at the top of the pane.

Workspace and File Expiration

If you want to expire your Workspace earlier than the limit set by the administrator, you can do so in the Web Transfer Client.

- If the EFT administrator has enabled link expiration, the ability to download the attachments will expire within the time specified.
- If the administrator has selected the **Retain files after link expiration** check box, the temporary Workspace is removed from the virtual file system in EFT, but the files are still available on disk until the "retain files" expiration date. This setting applies to file expiration (separate from link expiration) and affects Drop-Off portal, Send portal, Reply portal, and request-file methods of file delivery.
- In v8.3.0.2 and later, an expiration message appears in the Send and Reply portals:



To expire the Workspace

1. Select the Workspace (folder) that you want to expire.
2. On the tool bar, click **Edit Workspace**.
3. Specify the date that you want to expire the Workspace.
4. Click **OK**.

Related Topics

- Enable Send Portal
- Stop Sharing a Workspace
- Sharing Folders (Creating a Workspace)

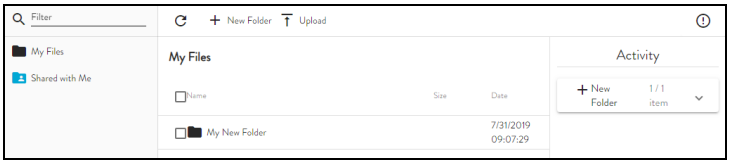
- Edit Workspace Permission
- Add Workspace Participants

Creating Folders

When you first log in to the Web Transfer Client (WTC), you are in the top folder that you are allowed to view. You can create sub folders within this folder, and those folders can have subfolders.

To create sub folders

1. In the folders pane, click to select the folder (for example, **My Files**) under which you want to create a subfolder.
2. On the toolbar, click **New Folder**.
3. Provide a name for the folder, then click **Create**. (Folder names follow standard Windows file naming conventions.)
4. The new folder appears in the right pane, and the Activity pane indicates that you created a new folder. (Click the information icon to open the Activity pane.) You can now move files between folders and upload files to the new folder.



Deleting a Folder or File

You can delete folders and files in your home folder and in subfolders.

To delete a file or folder

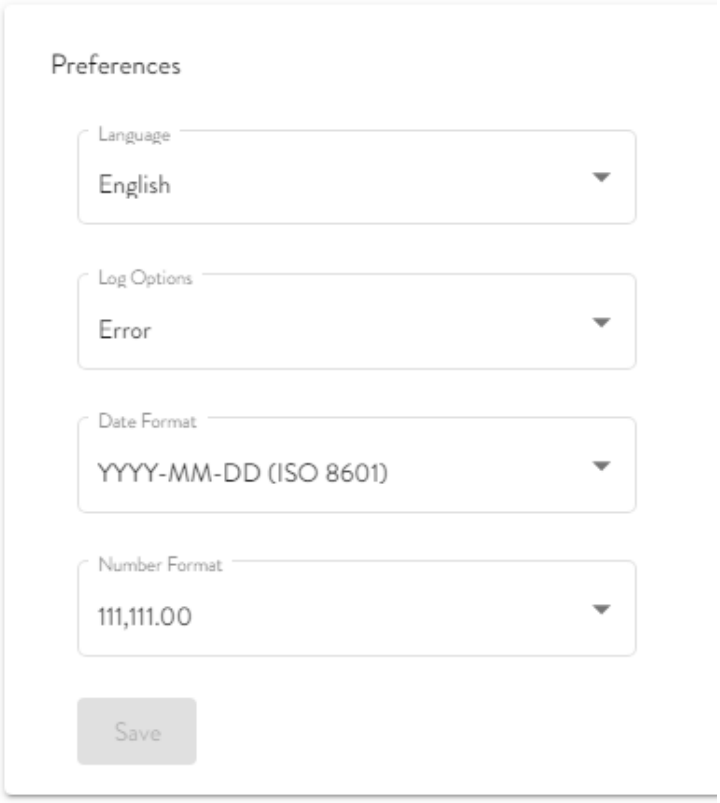
1. Select the check box for the file or folder that you want to delete.
2. On the toolbar, click the **Delete**icon.
3. The **Delete confirmation message** appears. Click **Confirm**. The file is deleted. There is no restore or undo option.

Change Your Profile

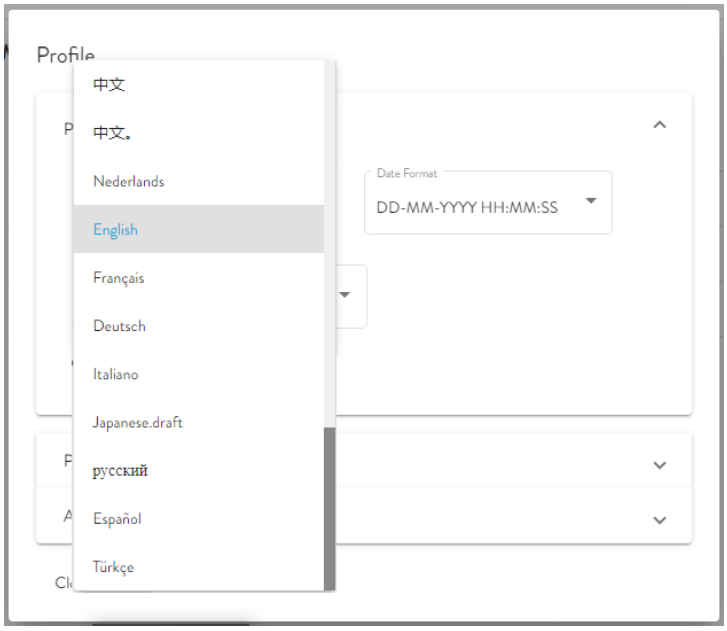
You can specify options for language, logs, data format, and number format in the **Profile**dialog box.

To change your preferences

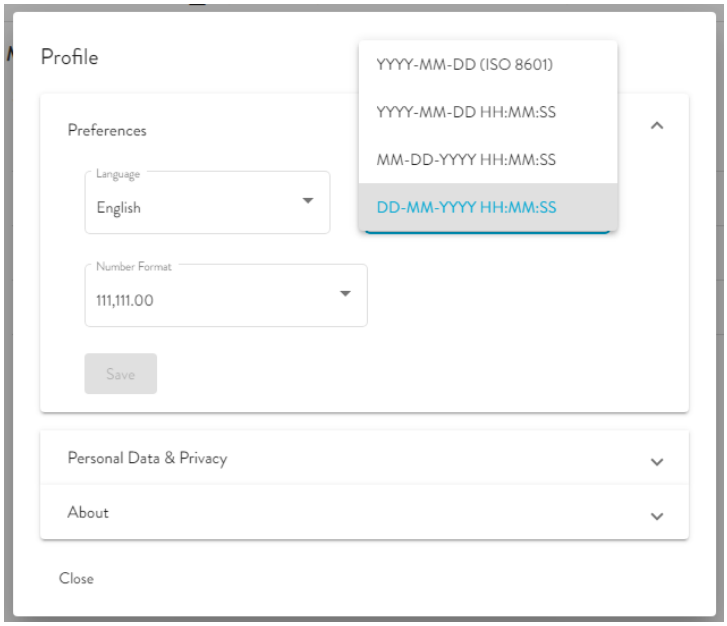
1. In the upper-right corner, click your login name, then click **Profile**.
2. Click **Preferences**.



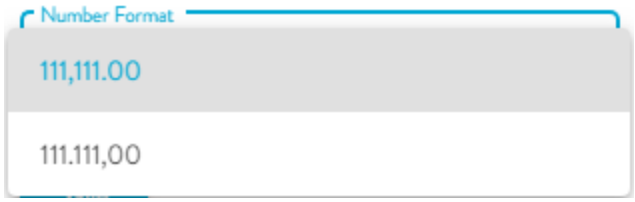
3. Click the drop-down arrow in each box to specify your preference.
    - Languages include English (default), 中文 (Chinese Simplified), 中文。(Chinese Traditional), Nederlands (Dutch), Français (French), Deutsch (German), Italiano (Italian), (Japanese), русский (Russian), Español (Spanish), and Türkçe (Turkish).



- Date Format options include YYYY-MM-DD (ISO 8601 format), YYYY-MM-DD HH:MM:SS, MM/DD/YYYY, or DD.MM.YYYY.



- Number Format options include 111,111.00 or 111.111,00



4. Click **Save**.
5. Click **Close**or anywhere outside of the dialog box to close it.

Refer to Personal Data and Privacy Settings for reviewing or editing your personal data or privacy rights.

Personal Data & Privacy Settings

In the **Profile** dialog box you can specify personal data and privacy settings. Before you can view or edit these settings, the EFT administrator must set various options on the **Site > Web** tab, in the **GDPR** dialog box (Article 3 and Articles 15 - 21).

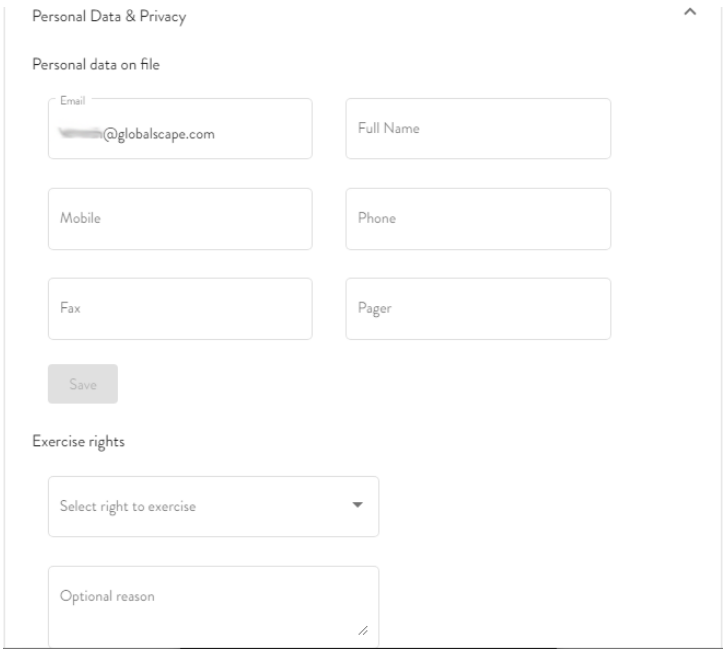
- If nothing is displayed when you expand **Personal Data & Privacy**, the EFT administrator has not configured that in the administration interface.
- Account details fields are not modifiable in the WTC for EFT users on an AD site.
- Account details fields are modifiable in the WTC for Guest users on an AD site.

When accessing EFT for the first time via FTP, FTPS, or SFTP, and the Privacy Policy consent is required for use, the connection will fail. The user must first connect via the Web Transfer Client (HTTPS portal) to consent to the policy. (The administrator can instead set the status for the Privacy Policy for a given user manually, on user account's **General** tab in the EFT administration interface.)

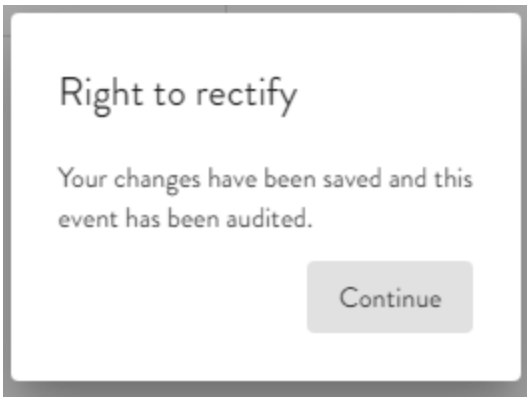
Depending on the privacy settings configured by the EFT administrator, restricting the use of your personal data (which can include your name and email address) may result in the **termination of the current session** to which you are logged in and the removal of your account from the server. If you are unsure about exercising your rights as described below, contact the administrator.

To change your personal data and privacy settings

1. In the upper-right corner, click your login name, then click **Profile**.
2. Click **Personal Data & Privacy** to expand the dialog.

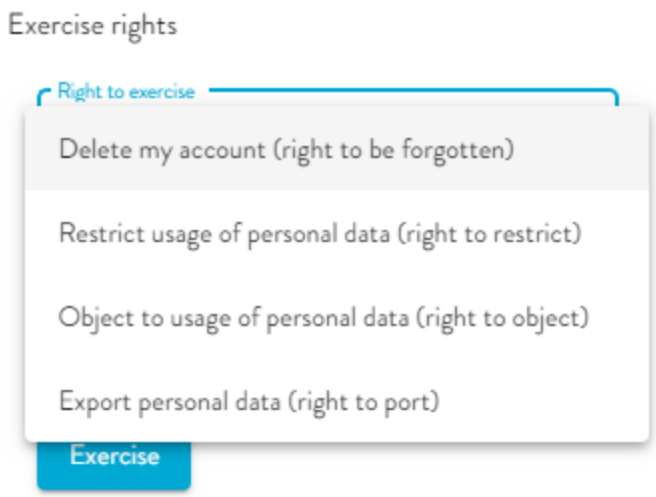


3. The **Personal data on file area** indicates which data is stored in EFT. By default the data is stored encrypted. If you change any of the settings, the **Right to rectify** message appears.

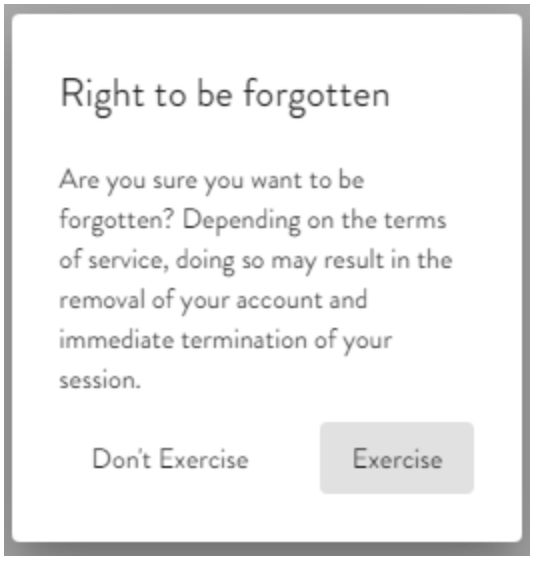


4. Click **Continue**, then click anywhere outside of the **Profile** dialog box to close it.

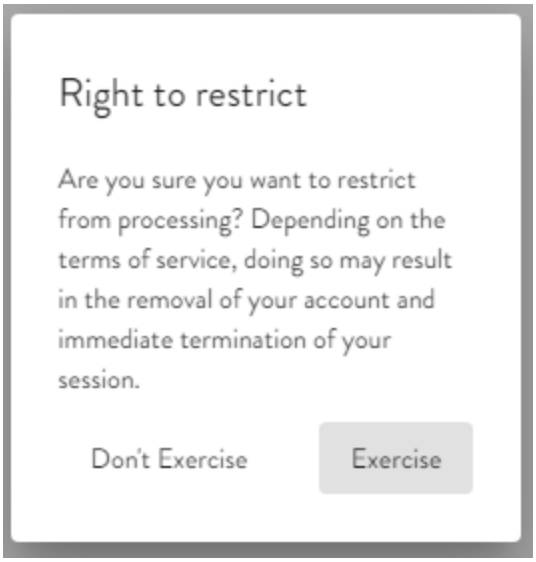
   The **Exercise rights** area enables you to exercise your rights to delete your account from the server, restrict use of personal data, object to use of personal data, and export your personal data. Each right is described below.



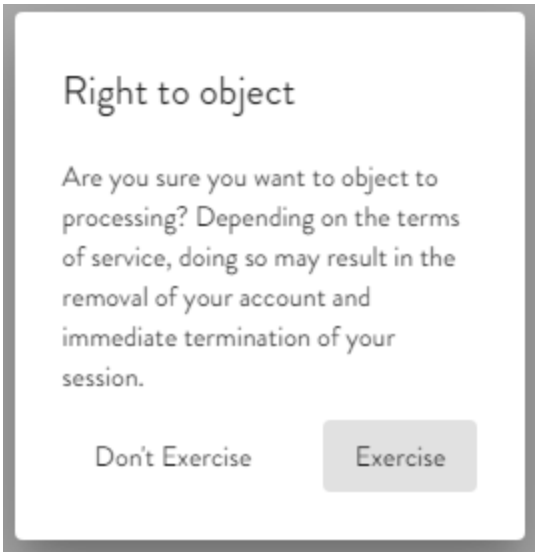
5. **Delete my account** - Depending on the Terms of Service, “forgetting” your account may result in the removal of your account and termination of the current session to which you are logged in. If you are unsure, click **Don't Exercise** and contact the administrator. Otherwise, click **Exercise**.



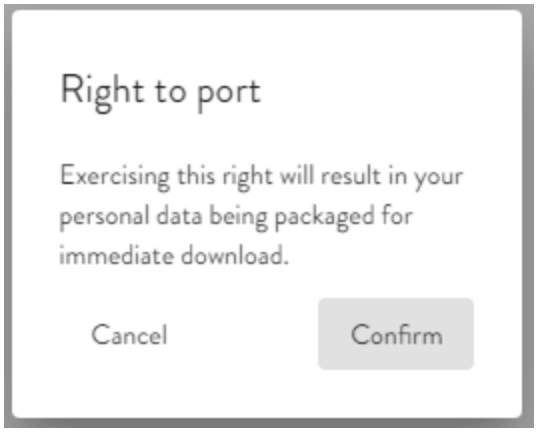
6. **Restrict usage of personal data** - Depending on the Terms of Service, restricting the use of your personal data may result in the removal of your account and termination of the current session to which you are logged in. If you are unsure, click **Don't Exercise** and contact the administrator. Otherwise, click **Exercise**.



7. **Object to usage of personal data** - Depending on the Terms of Service, objecting to the use of your personal data may result in the removal of your account and termination of the current session to which you are logged in. If you are unsure, click **Don't Exercise** and contact the administrator. Otherwise, click **Exercise**.



8. **Export personal data** - This option packages your data in a JSON (text-based) file and saves it to the Downloads folder specified in your browser. You can review the file in any text editor, such as Notepad.



9. Click **Confirm** to begin the download.
10. Click **Close** or anywhere outside of the **Profile** dialog box to close it.

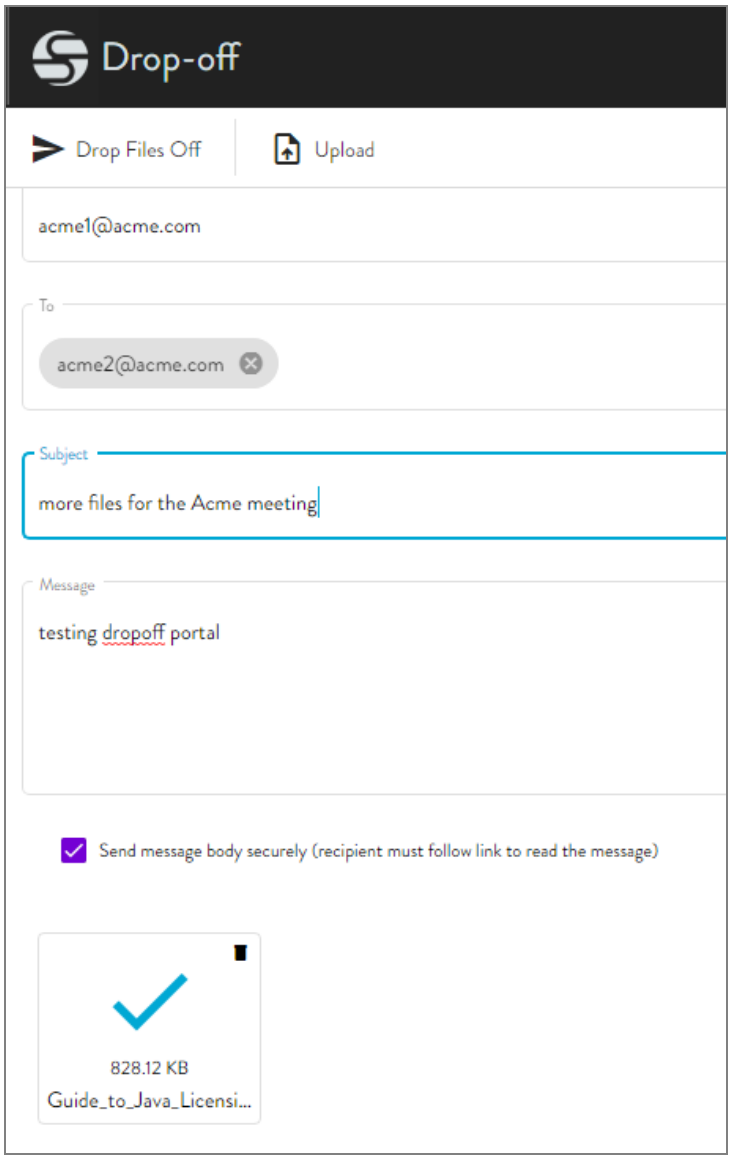
Drop Off Page

The Drop-Off page can be used by external users to send files to internal users on demand (ad hoc), without creating user credentials.

- **A Workspaces license is consumed for each Drop-off page message**no matter how many recipients the message has. A license is not consumed on replies. A license is not consumed on Send messages. You can avoid Workspaces licenses being consumed by the Drop-off page by disabling the Drop-off page. It is not enabled by default.
- When someone uses the Drop-off page, that person becomes a "Workspaces owner." This is because behind the scenes, a temporary, anonymous account is created to host the Workspace, thus consuming a license (assigned to that account). Once the space expires, the anonymous account is also removed, and the license is released to the pool.

To send a file using the Drop-Off page

1. In your browser, go to the URL provided. The Drop-Off page appears. (Your administrator or an internal user will provide the address. URL can be found on the **Site > Web** tab in the Drop-off page configuration.)



2. In the **From**box, provide the email address at which you want to receive responses.
3. If the **To**box is enabled, you are limited to addresses in the domains defined by the administrator or to lists defined in the EFT administration interface.
4. In the **Subject**box, provide a clear topic of the email. (that is, "Files for Wednesday's Acme project meeting" is clearer than "The files you wanted.")
5. In the **Message**box, provide a brief reason for the email.
6. Drag and drop or click **Upload**to select files to attach to the email. If CAPTCHA is enabled, you must complete the CAPTCHA before you attempt to attach files to the portal. Otherwise, the files won't attach.
7. (Optional) To send the request securely, select the **Send message body securely**check box.

8. Click **Drop Files Off**. A confirmation message appears.
9. If you want to send another file, click **Do it Again**. If the send was not successful, an error message appears. Click **Try Again** to verify the email address and resend the email.
10. The recipient will receive an email with a download link. If the recipient has an account on EFT and signs in to the Pick-Up page, the recipient can reply to the sender.

Pick Up Files

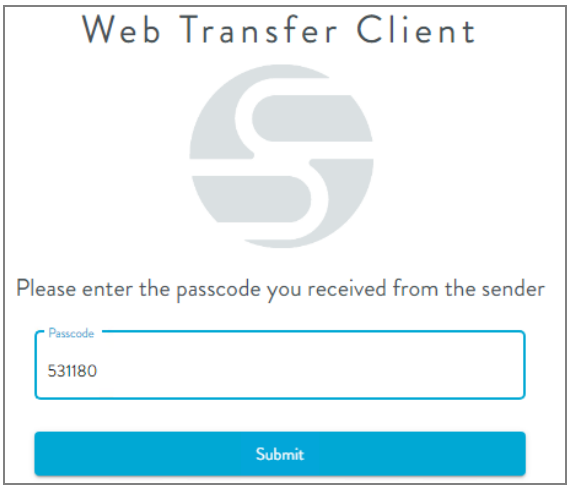
After a Workspaces or EFT Outlook Add-In user sends one or more files, the recipients can click a link in the email that they receive that opens their default browser to the Workspaces Pickup page.

Depending on the administrator's settings, the files might be available for download only once, after which the download links will expire. (If the administrator has selected the **Retain files after link expiration**check box, the files are available on disk until the "retain files" expiration date.)

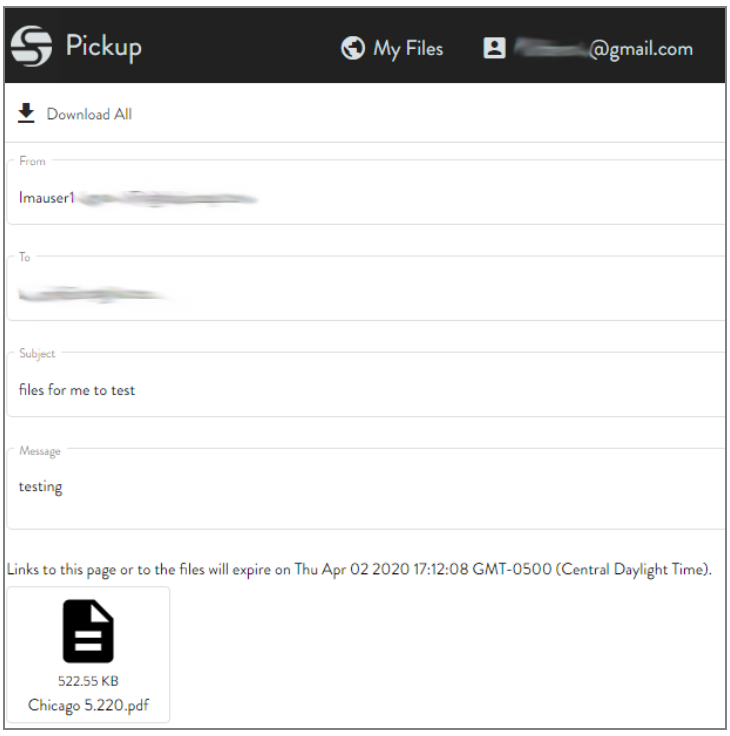
In certain browsers, if you are using a self-signed certificate you will receive a "network issue" warning when downloading files. Workarounds are to have a valid certificate, use special flags to ignore improper certificates, or not use HTTPS.

To download files in the Pickup page

1. In the notification email, click the **Workspace**link. The default browser opens.
2. If the sender has specified password-protected pickup, a login page appears. The sender should have sent you the passcode in a separate email, text, or phone call.



3. Provide the passcode, then click **Submit.**



4. Select one or more files and click **Download Selected** to download multiple individual files or click **Download All** to download all of the files. The files are saved in the browser's downloads location.

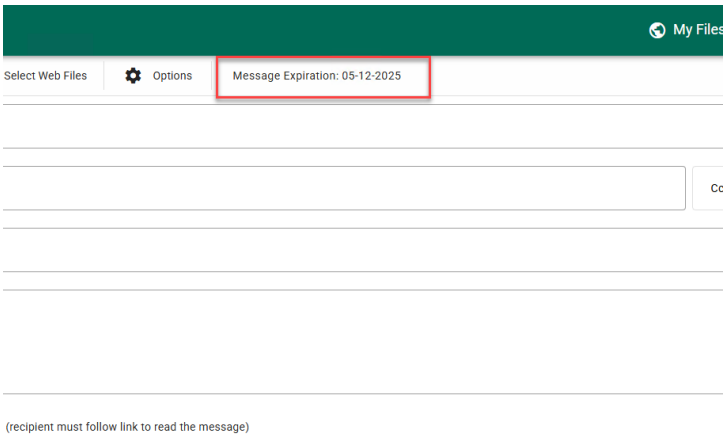
Reply to Messages

After you have received a message sent through Workspaces, you can reply to the email (if so configured) and send files back.

> **NOTE:** The Send and Reply portals must be configured by the EFT administrator.

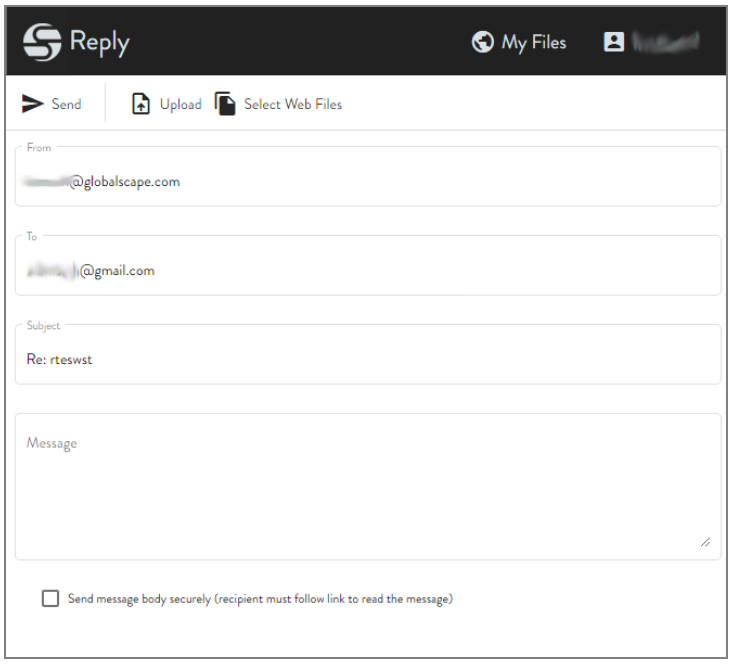
Reply and **Reply All** buttons are displayed under the following conditions:

- For anonymous recipients, if the sender has enabled replies
- For authenticated recipients:
  - if the Workspaces license limit is not exceeded (during trial)
  - if Allow recipients to reply check box has selected (by administrator)
  - if Workspaces and Send Files are both enabled (by administrator)
- **Reply All** button is not displayed if sender is the only available recipient on the thread.
- The alias name is displayed if any recipient is from an alias list
- In v8.3.0.2 and later, and expiration message appears in the Send and Reply portals:



To reply to the email

1. Click the **Workspaces**link in the email. The **Pick Up** page appears.
2. Click **Reply**. The **Reply** page appears.



3. The **From**, **To**, and **Subject** lines are completed for you. Compose a **Message**, "drag and drop" or browse for files, then click **Send Message**.
4. If the reply is in response to a request for files, the **Send message body securely** check box appears.
5. Complete the email and click **Send**.

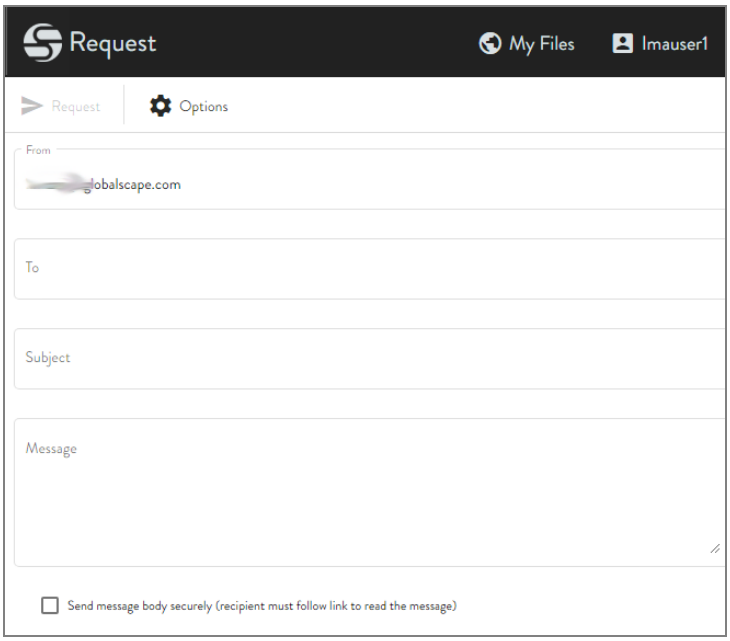
Request Files

In the Web Transfer Client, a user can request files from another user if Workspaces is enabled to send files.

> **NOTE:** Both the Send and Reply portals must be enabled to request files.

To request files

1. Click the **Request Files**icon. The **Request Files** window appears, and the **From** address is completed for you.

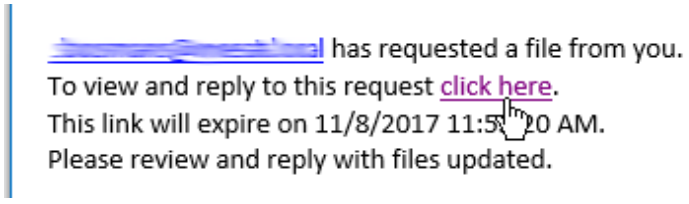


2. Provide the **To** address, **Subject**, and **Message**.
3. To send the request securely, select the **Send message body securely** check box. In this case, the recipient will have to click a link to read the message, instead of the message being displayed in the email.
4. Click **Options**.

a. Under **Authentication**, specify whether you want the recipient to log in to download the file. If you click **Authentication not required**, you also have the option to select **Unauthenticated users can respond**to the email. When the check box is not selected, an unauthenticated user can download the file, but cannot respond in the portal.
b. Under **Message Expiration**, specify how soon the message is to expire: 1 day, 1 week, 1 month, or immediately. (See note below about expiring immediately.)
c. Select the **Save as Default**check box if you want to save these options for future file sends.
d. Click **Set Options**to save your settings.

5. Click **Apply** to accept Request Options.
6. Click **Send Request**.

   The recipient will receive an email similar to the one below. The last line is the Subject line of the request email.



7. The recipient should click the "click here" link to open the Reply portal in which the recipient can attach the requested files to send to the requestor.

   If the message is set to immediately expire, do not leave the page or click refresh without responding or attaching the requested files. If a recipient clicks on the link and then clicks refresh, all the fields go blank. If the user clicks the link in the request file email again, then they are presented with a "404 object

not found" error and you will have to inform the requestor to send their request again (or send the files via other means).

8. The recipients can view their received messages by clicking **Received Messages** in the left pane.

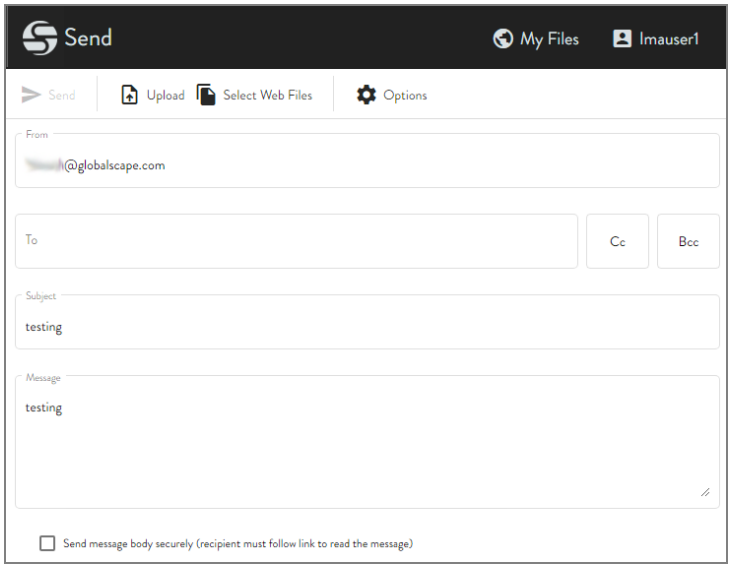
Send/Email Files in Workspaces

EFT users who want to add files that are either located in their local machine or are in Workspaces can do so securely. Recipients of those files can pick up the files in their default browser.

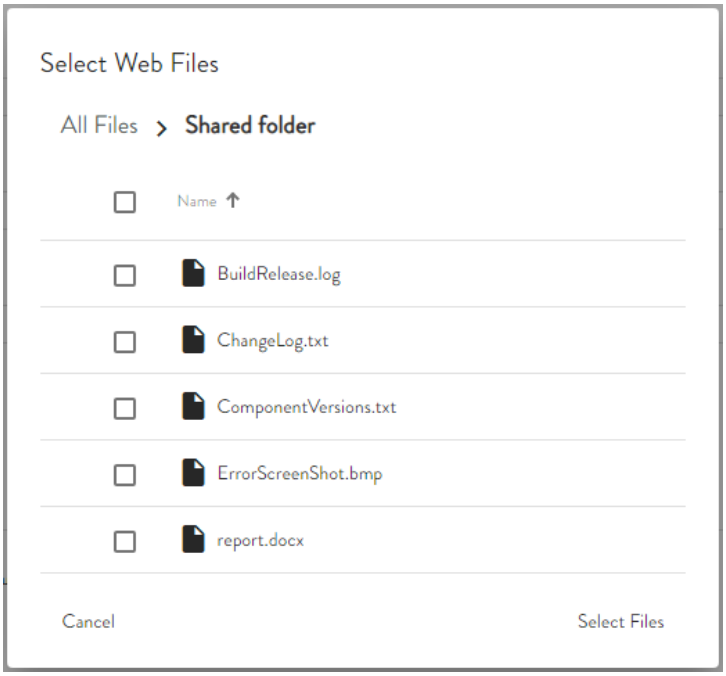
- The browser will timeout after a period of inactivity. Files that are being uploaded are considered "activity." Idle timeout occurs if you leave the browser open and stop composing your message with no activity. Upon timeout, the draft is lost. An "about to timeout" warning prompt is displayed when timeout is imminent, giving you the opportunity to keep the session alive.
- When you send a file using Workspaces, a "WorkspacesSendMessage" folder is created in the Virtual File System (VFS).
- You can send a secure message in Workspaces without an attachment, however, you cannot expire the message immediately without an attachment.

To email files

1. Log in then click the **Send** icon on the toolbar. The **Send files securely** form appears.



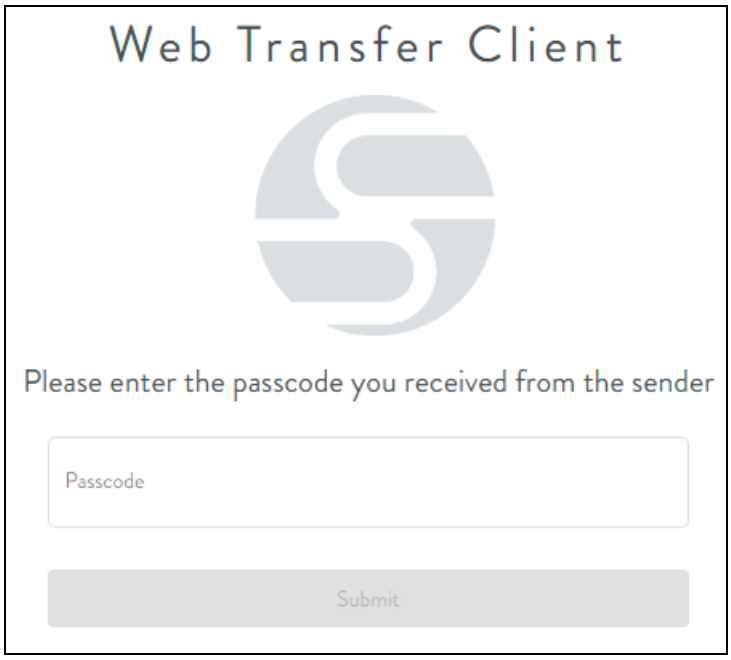
2. To attach files, drag and drop them on to the page, or click **Upload** or **Select Web Files**.
    - If you click **Upload**, the Windows **Open** dialog box appears for you to select your files, and then click **Open**.
    - If you click **Select Web Files**, the **Select Web Files** dialog box appears.



- Specify the folder that contains the file(s) you want to send, then select the files, and click **Select Files**.

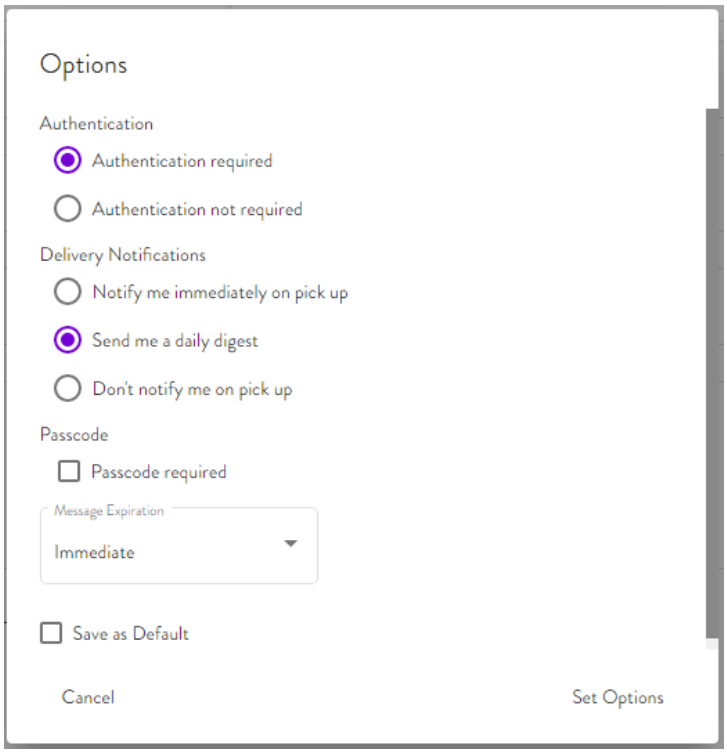
3. Select the **Send message body securely** check box to send a secure message. In this case, the recipient will have to click a link to read the message, rather than the message being displayed on the Pickup page.
4. Select the **Passcode required**check box if you want the recipient to provide a passcode to download the file.
   - When this check box is selected, after you click Send, an automatically generated passcode appears.

   - Send the passcode to the recipient in a separate email, text message, or phone call. When they click the link to download the file, a passcode message appears.



- The recipient must enter that passcode to be able to download the file.

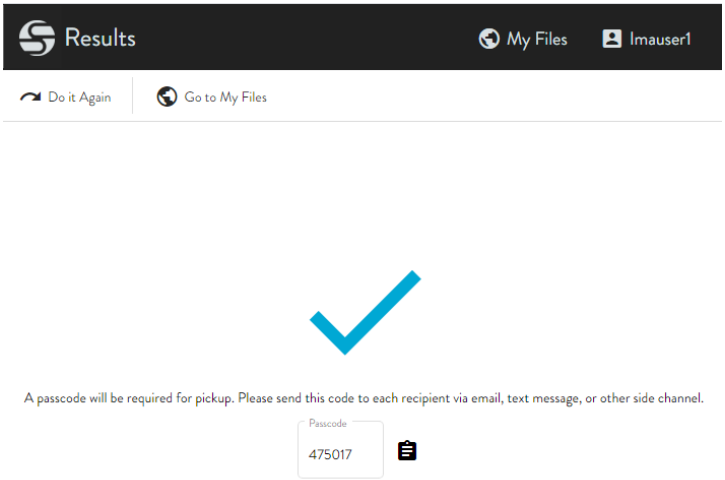
5. To specify message options, click **Options**.



6. Under **Authentication**, specify whether you want the recipient to log in to download the file. If you click **Authentication not required**, you also have the option to select **Unauthenticated users can respond**to the email. When the

check box is not selected, an unauthenticated user can download the file, but cannot respond in the portal.

7. Under **Delivery Notifications**, specify If and when you want to be notified when a file you have sent is downloaded.
8. Under **Passcode**, select the **Passcode required**check box if a passcode is required to download the file.
9. Under **Message Expiration**, specify how soon the message is to expire: 1 day, 1 week, 1 month, or immediately. In v8.0.2 and later, you can send a secure message without an attachment, however, you cannot expire the message immediately without an attachment. (The dialog box does not display the date it will expire.)
10. Select the **Save as Default**check box if you want to save these options for future file sends.
11. Click **Set Options** to save your settings.
12. Click **Send**. A message appears indicating whether the message was sent successfully or not.
13. If you selected the **Passcode required** check box, after you click Send, a **Results** page appears and displays the passcode that your recipient will need to pickup the file.



   - Click the clipboard icon to copy the passcode to your clipboard, then paste the code into an email or text message or other side channel.

The **Not Sent** message appears if you have EFT configured to send only to EFT users (most restrictive) and you try to send to non-EFT users. If you need to send to user accounts that are not defined in EFT, your EFT administrator will need to either change the setting on the **Web**tab of the EFT Site, or add the account as an EFT user.

14. If sending the message was successful, the recipient(s) receive an email with a link to pick up the files.
15. The items that you send will appear in the **Sent Messages** view. This includes messages sent to request files.

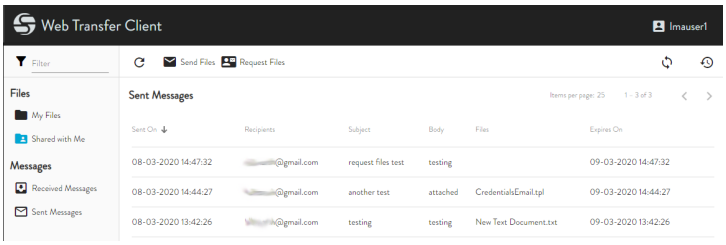
Related Topics

- Picking Up Files
- Drop-Off Portal
- Joining a Workspace
- Sharing Folders (Creating a Workspace)
- Managing Workspaces in the VFS
- Request Files
- Reply Portal

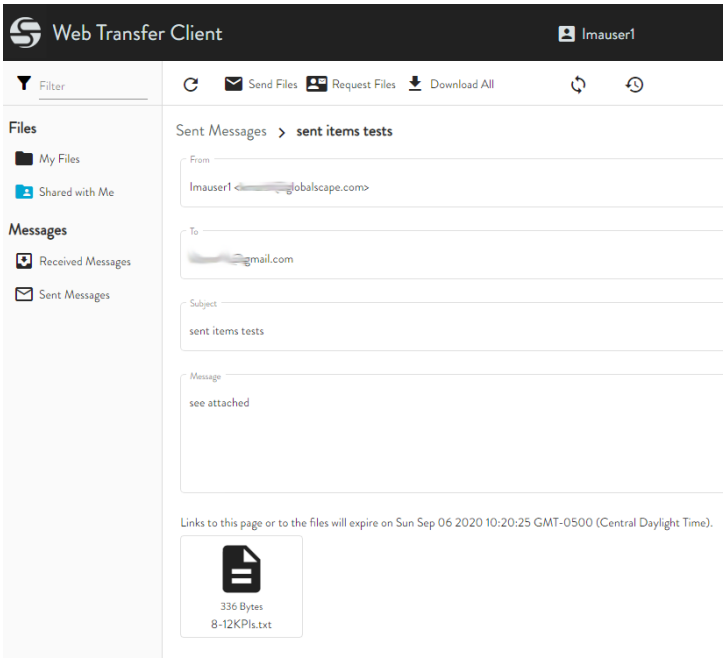
Viewing Sent Messages

Workspaces users can view a list of the messages they have sent, and their attachments. Once the items expire (if the EFT or user have set an expiration), those items are no longer viewable.

- The last 50 items that you sent will appear in the **Sent Messages** view. (Configurable by the administrator using an Advanced Property, **BigCollectionsPageSize**.)
- The list includes messages sent to request files.
- The column width is limited to 101 characters and no more than 4 filenames and 4 recipients.



- As shown above, the messages are listed by and can be sorted by the **Sent On** column. Click a message to open it.

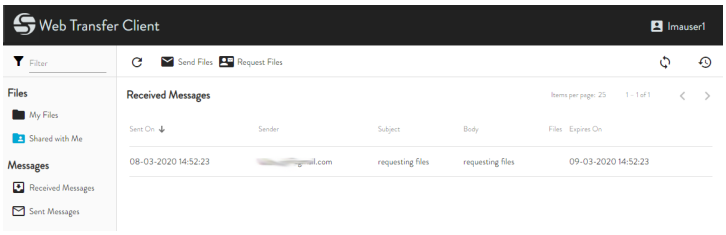


- You can download the attachments on a message, and they are saved in your browser's Downloads folder.
- Expired items are removed immediately and not able to be viewed in Sent Messages window.

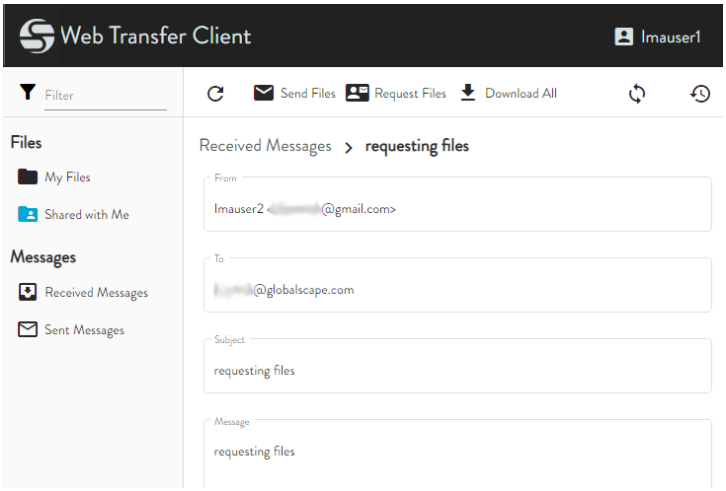
Viewing Received Messages

Workspaces users can view a list of the messages they have received, and their attachments. Once the items expire (if the EFT or user have set an expiration), those items are no longer viewable.

The recipients can view their received messages by clicking **Received Messages** in the left pane. A list of received messages appears.



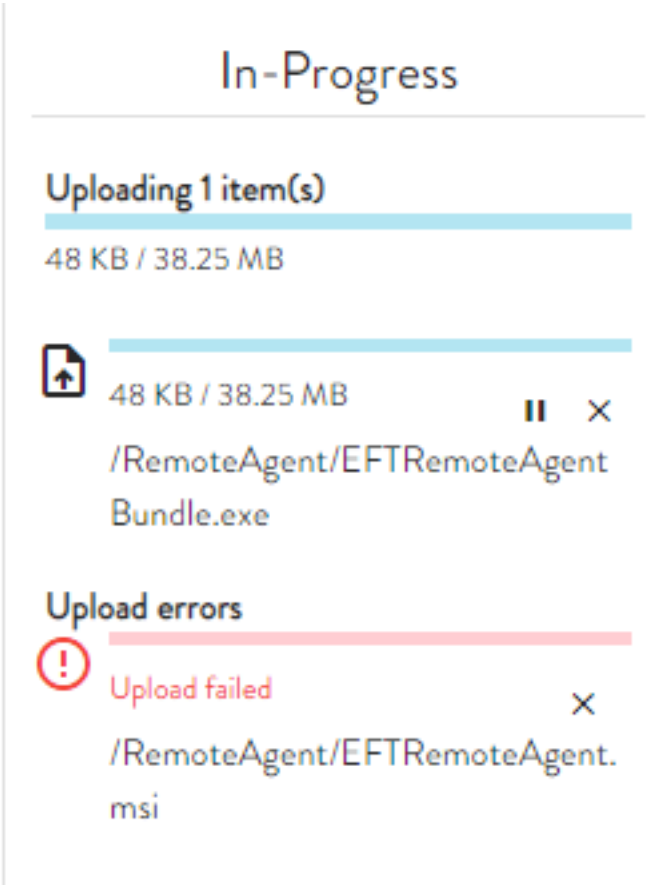
- As shown above, the messages are listed by and can be sorted by the **Sent On** column. Click a received message to view the message.
- EFT will return the last 50 records of ad hoc transactional data. An advanced property, **BigCollectionsPageSize**, can be set for more or fewer records.



- Download the attachments on a message by clicking **Download All**. If an expiration was set, the expiration date and time appear at the bottom of the message.
- Expired items are removed immediately and not able to be viewed in Received Messages window.

Viewing Transfer Status

A Workspace owner or a participant can view the progress of files being transferred in Workspaces. Once the transfer is completed, the transfer status goes away, but the **In-Progress**panel remains open. If the transfer failed, the **In-Progress**panel displays which transfer failed. The client will remember the last state (open or closed) of the pane.



To view a Workspace's in-progress transfers

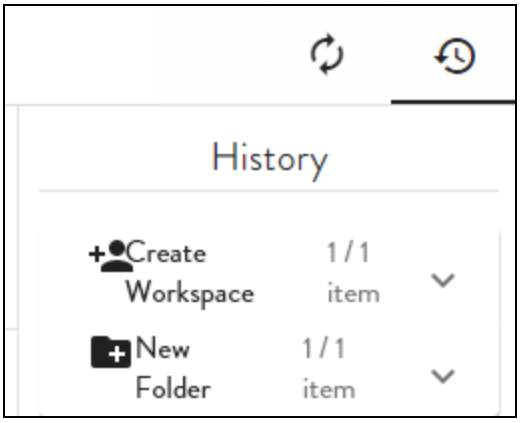
1. Before uploading or downloading files, open the **In-Progress**panel by clicking the rotating arrows icon .
2. Initiate the transfer. The progress will appear in the panel. Note that smaller files will barely display before completing.

View Workspaces History

A Workspace owner or a participant can view a consolidated list of transactions (History) related to the Workspace.

To view a Workspace's history

1. Click the History icon in the upper right. The actions that have occurred while your session is open will appear here. If you send a file and then click Go back to My Files, the History panel is cleared.



2. As the **owner** of the Workspace, you can view your activities and participant's activities:
    - A Workspace **owner**can view a list of Workspaces operations for Workspaces you created (own), regardless of the initiator of that operation

    A Workspace **participant**can view a list of Workspaces operations by selecting the check box next to the shared folder, then click **View Workspace**. The **View** dialog appears and shows the operations that the owner or they initiated, depending on whether it is a public or private workspace:

    - **PUBLIC** Workspaces that they are members of, regardless of the initiator of that operation
    - **PRIVATE** Workspaces that they are members of, only for operations initiated by them or the owner

    The icons to the left of each item provide a quick glance of which operation was

performed:

- When a workspace is deleted, the history records related to that workspace are removed. The files within the folder that is deleted (or moved) are not recorded separately in history as deleted (or moved).
- When a participant leaves a workspace (but the workspace remains), the user no longer has access to new or historical records for that workspace.
- When a participant joins workspace after some period since creation, they will see historical records for that workspace since its inception.
- Resending a workspace invitation is recorded as a send.

- When an EFT administrator adds participants to the workspace in the VFSin the EFT administration interface, the history for that workspace displays an entry for each user as "modified" because the workspace itself was modified by the addition of that user.

Edit Notification Options

When you create a Workspace, you can specify how often you want to be notified regarding actions taken on the Workspace, such as when files are uploaded to your Workspace.

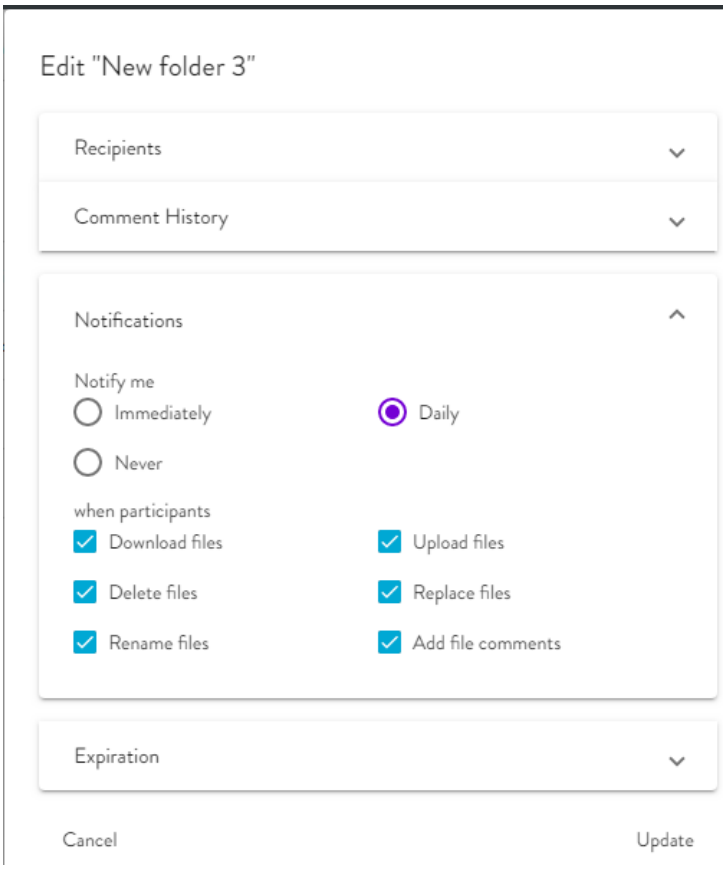
In the **Notifications** area, you can:

- Receive an email immediately after every action is taken
- Receive an email of all actions that were taken that day (sent at 12 am)
- Never receive emails on actions taken.
- Choose specific actions to be notified about, or none at all.

If you later want to change your notification settings, you can do so in the **Edit Notifications Options**dialog box.

To change notification options

1. On the toolbar, click **Edit Workspace**. The **Edit Workspace**dialog box appears.
2. Expand the **Notifications**area.



3. Make your changes and then click **Update**.

Related Topics

- Stop Sharing a Workspace
- Editing Workspaces Sharing
- Managing Workspaces in the VFS
- Transactional Workspaces
- Workspaces Invitations
- Workspaces Notifications

Notifications

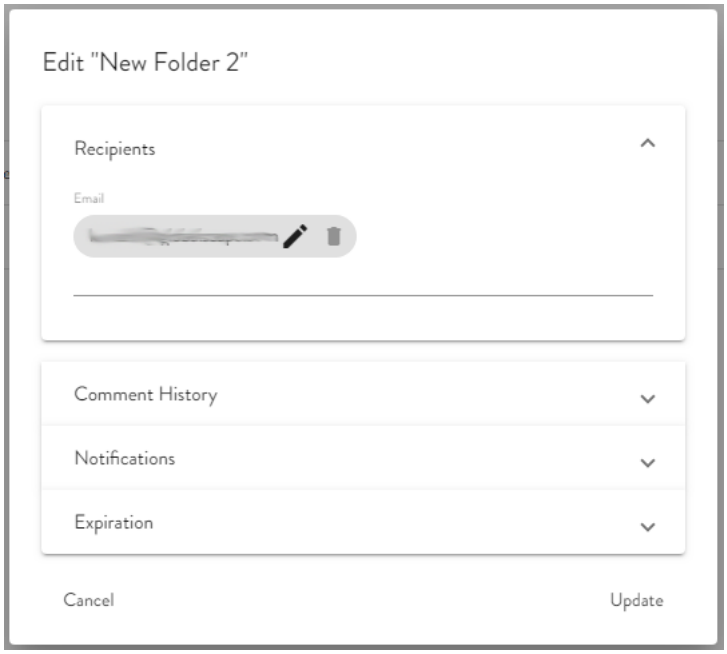
Each Workspace participant can configure notifications to let them know when actions are performed on the Workspace, such as uploading or downloading. The notifications are set to Daily for all actions by default.

The Workspaces owner is notified when the specified actions occur, in the form of:

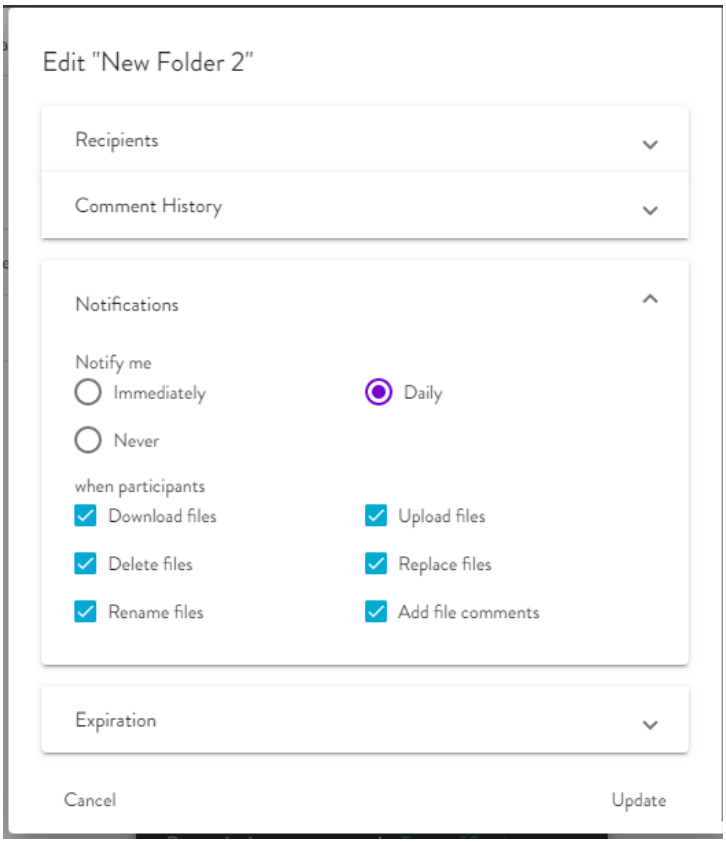
New Folder 2: EFT_HighAvailability_Datasheet_es-MX.docx was uploaded by Imauser2 from 127.0.0.1 on 8/28/2019 at 11:24:29 AM.
New Folder 2: EFT_HighAvailability_Datasheet_es-MX.docx was renamed by Imauser2 from 127.0.0.1 on 8/28/2019 at 11:25:03 AM.

To enable notifications

1. Select the check box for the folder for which you want notifications.
2. Click Edit Workspace. The **Edit** dialog box appears.



3. Expand **Notifications**.



4. Specify the notification frequency (the default is daily) and which actions to be notified about (all are selected by default).
5. Click **Update** to save your changes.

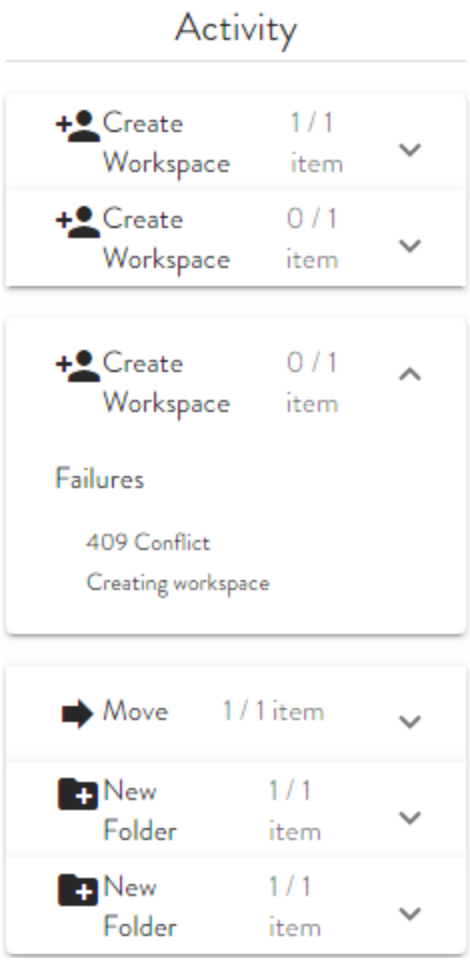
Messages

Messages and prompts appear for a variety of scenarios in the Activity pane. Click the down arrow next to the item for more information.

For example:

```
409 Conflict Creating workspace
```

means that there was a problem creating the workspace.



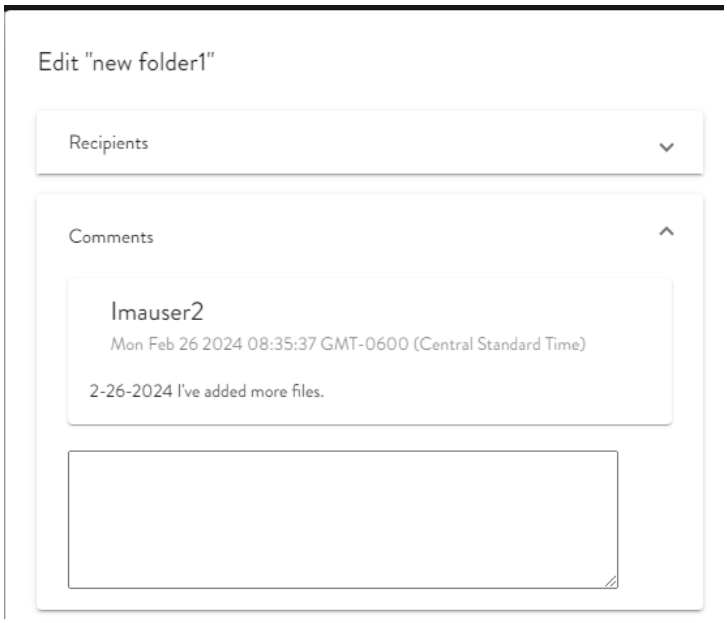
Workspaces Comments

You can add comments to a shared Workspace. You can also view the comments that have been added. All participants in this shared folder can read the comments.

To view or add comments to a shared Workspace

1. Click the check box next to a shared folder.
2. The toolbar updates to show more options. Click **Edit Workspace**.

3. Expand the **Comments** section. If no comments have been added, the **Comments** box is blank.



4. To add comments, type in the text box, then click **Update**.

File-Naming Conventions

EFT follows the standard Windows naming conventions, with a few exceptions. (Please refer to Unicode File Transfers and Unicode Exceptions for details of using Unicode characters.)

For example:

- You can name files using almost any character for a name, except for the following reserved characters: **< > : " / \ | ? * %**
- The maximum length for a path is 255 characters. This limitation includes the drive letter, colon, backslash, directories, subdirectories, filename, and extension. If the relative path is too long, a warning message appears. (To change the path-length limit, refer to Maximum Path Length Lion in Microsoft Learn.)
- Characters that are valid for naming files, folders, or shortcuts include any combination of letters (A-Z) and numbers (0-9), plus the following special characters.

^	Accent circumflex (caret)	$	Dollar symbol	(	Parenthesis opening
&	Ampersand	€	Euro symbol	)	Parenthesis closing
'	Apostrophe (single quotation mark)	=	Equal sign	.	Period
@	At symbol	,	Comma	+	Plus
{	Brace left	!	Exclamation point	~	Tilde
}	Brace right	-	Hyphen	_	Underscore
[	Bracket opening	#	Number sign		
]	Bracket closing	%	Percent		

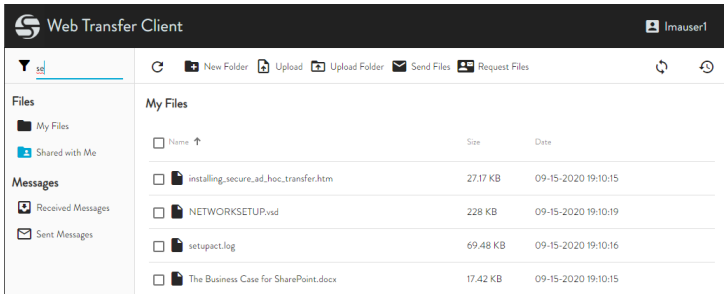
NOTE: For more information regarding file-naming conventions, refer to the *Microsoft Windows Developer Network* article *Naming a File* and the *Microsoft TechNet* article How NTFS Works.

Filtering and Sorting the File List

You can filter the display of the files to display only the files that you want by name or file size. Additionally, you can sort the **File Name**, **Size**, and **Date**columns by clicking the arrows in the header. Note that if you filter for the letter *b*, you will see ALL of the files since every file has MB, KB, or GB in the **Size**column.

To filter or sort the file listing

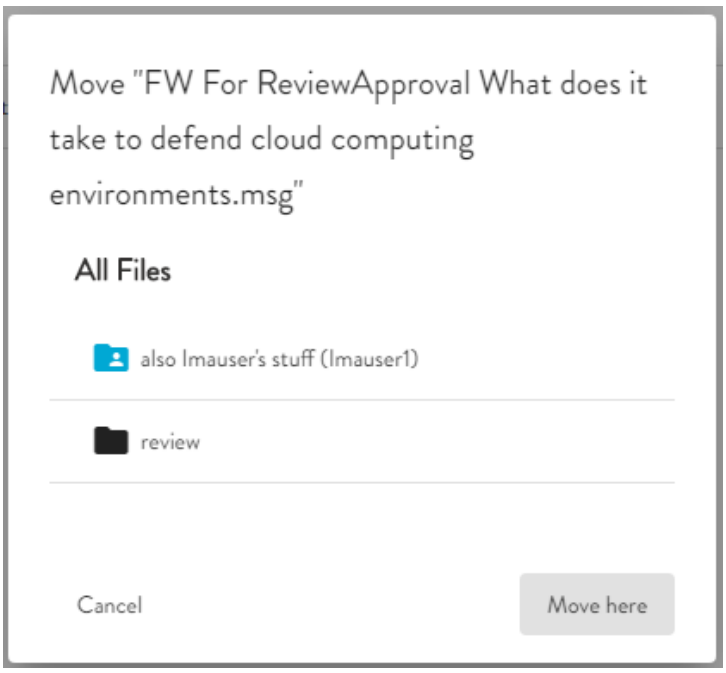
1. Click in the **Filter**box in the upper left, then start typing the name of the file you are looking for.



2. After two characters are typed, the file listing will update to display only files that contain the letters you've typed. Continue typing to narrow the listing. You can also filter by file size.
3. To refresh the file listing, click the **Redo**icon .
4. **To sort the list alphabetically,** click **Name**at the top of the list.
5. **To sort the list by size or date**, click **Size**or **Date** at the top of the list.

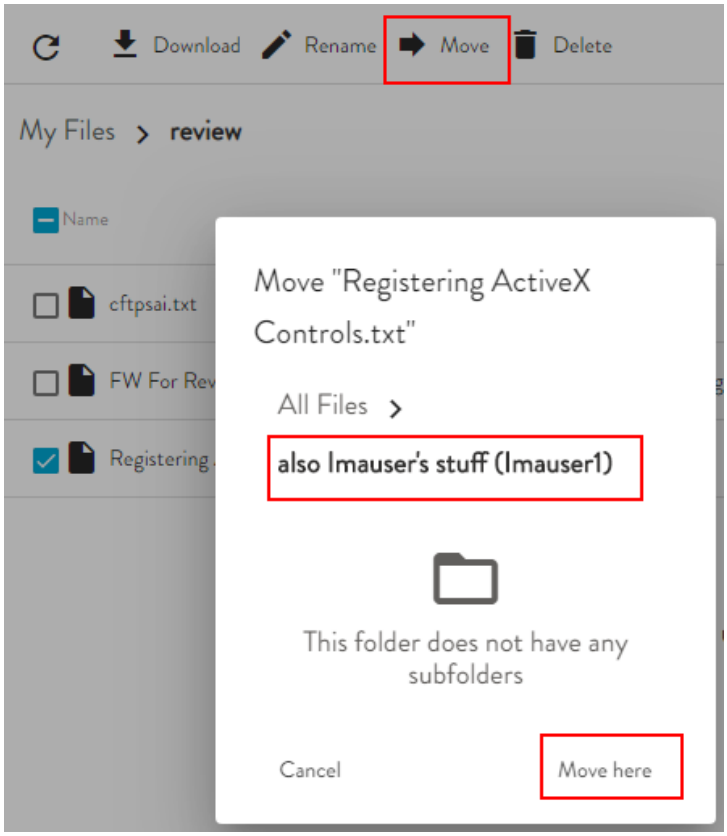
Moving Files between Folders

After you have created subfoldersin your home folder, you can move files between those folders. Users with whom a Workspace is shared who have permission to move files and folders out of the Workspace can move files between Workspaces. For example, lmauser1 shares a Workspace with lmauser2. lmauser2 can move files from their file list to the shared Workspace folder (indicated by the Shared icon and the username appended to the folder name).



To move one or more files to another folder

1. Select the check boxes of one or more files that you want to move, then click the **Move**icon. The **Move** dialog box appears.
    - The **Move**icon is visible even if you don't have permission to move files.



2. Click the folder to which you want to move the file(s), then click **Move Here**.
    - When**moving large files**, if a message appears saying that it failed to move the file(s), wait a minute to see if the file(s) appear in the folder.
    - When **moving folders** from one virtual directory to another, the "move folder" operation temporarily disables timeout checks (similarly to some other potentially time-consuming operations like CRC calculation or ZIP download). This is done to prevent EFT from closing the connection while the client waits for the server to complete the move. There is no progress bar; at times you will see the folder/files duplicated across the folders until the transfer is complete. (You will need to refresh the browser. Some browsers require that you clear browsing history completely before displaying an updated page.)

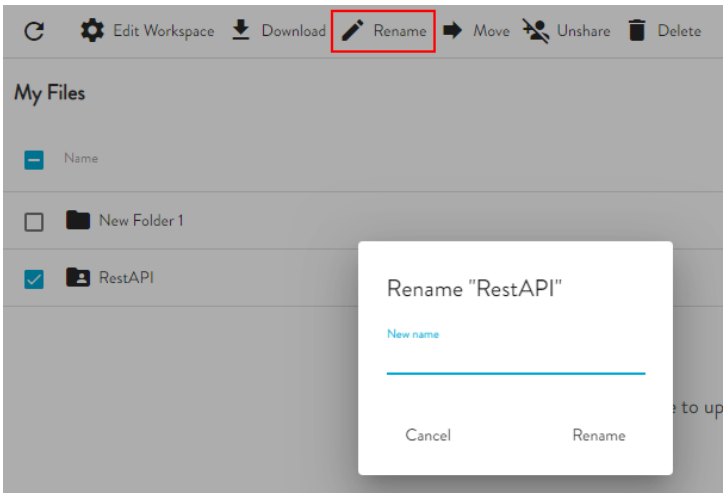
Renaming a File or a Folder

You can rename folders and files in your home folder and in subfolders. The WTC follows Windows file-naming conventions. That is, the following characters are invalid for file naming:

< > : " / \ | ? * %

To rename a file or folder

1. Select the check box for the file or folder that you want to rename.
2. On the toolbar, click the **Rename**icon.



3. The **Rename**dialog box appears. Provide a new name, then click **Rename**.

Searching for Files

If you have a large number of files and subfolders, you can find file more quickly by using filtersto search by name, size, or date, or typing text in the **Filter**box to find the file.

The **Filter** box merely matches the text string that you type. For example, it doesn't know the difference between a PDF file and a PNG file; however, if you type png, the search results will show all files with png in the file name, including the extension). It is not case sensitive.

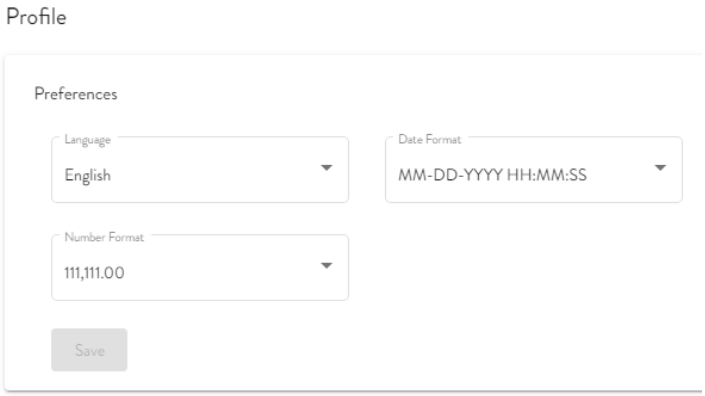
Certain wildcardswill return matching results. For example, **w*n**displays results that have a **w**, one or more other characters, and then an **n**, such as **W**EB_VP**N**_ Instructions.docx and **Wi**ndowsClustering.pdf. Wildcards are useful, for example, for finding files when you aren't sure how they were named.

To search for files using a filter

1. In the Filter box, type your search term and then press ENTER. As you type, the WTC will find matches for what you have typed.
2. Click the found item to navigate to it.
3. Click the icon on the toolbar for what you want to do with the file (download, rename, delete, move, etc.).

Language Settings

- In your Workspaces profile you can specify the language that you want to use for the main portal. Click your username in the upper right to open your Profile, then under **Preferences**, chose your language and click **Save**.



- The Workspaces registration page will attempt to detect the user's language stored in the browser's settings, if a supported language is detected. If the language is not detected, the page will default to English. This is the setting that is used in the Send, Reply, and Drop-Off portal.
    - **In Firefox**, the language setting will not keep the setting after logging out and then back into the browser.
- Or, on the **Registration**page, you can click the English drop-down list to choose other supported languages.

Web Transfer Client Pagination

The Web Transfer Client (WTC) directory listings can appear on multiple pages. The WTC will pull 500 records (folders/files) on initial load by default. WTC file listings have buttons for next page, previous page, and so on.

These pagination controls are only displayed when there is enough data to be paginated. If the page size is 500 and there are 1000 records, the controls will be displayed. However, if the page size is 500 and there are only 200 records, the controls will not be shown.

- When clicking "select all" in the table, the WTC will only select items that have been loaded. Changing pages will clear your selection.
- Filtering will only affect the items that are on the currently loaded page. This means that, if you have 500 items loaded out of 5,000 total, the filter operation will only be looking at the 500 items that are loaded at any given time.

The **fileListingDisplayLimit** advanced property in the **admin-configuration.json** file can be used to change the page display limit. If administrators want to turn off this functionality (that is, never use pagination for file listings), they should set this value to 0, which means there is no limit.

When retrieving listings from EFT, folders and workspaces are always given higher priority than files.

Logging Out

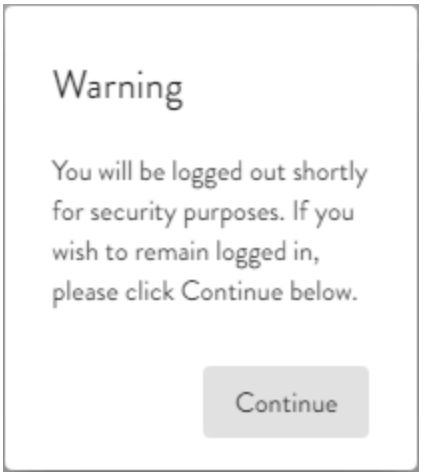
The server ends the session immediately when the browser is closed or after a period of inactivity. When the session is ended, the directory listing and any other personal information is cleared, and the login page is displayed.

To log out

- Click the username in the upper right corner, then click **Log out**. The WTC closes and the **Log In** page reappears.

Automatic Log Out

After a period of inactivity (approximately 10 minutes), a message appears warning that you are about to be logged out. You can click **Continue**to stay connected. The message will reappear for each period of inactivity.



WTC & Workspaces Administration

The topics in this section describe administration of the Web Transfer Client (WTC) and Workspaces.

- Workspaces Administration Overview
- Workspaces Licenses
- WTC Admin-Configuration Settings
- Allow Users to Create Workspaces
- Changing the Language of the Client
- Changing Logo or Colors in the WTC
- Disable CRC
- Display Full Name of User in WTC on LDAP Site
- Enabling User Access to the Web Transfer Client
- Enable and Configure Folder Sharing (Workspaces)
- Enable and Configure the Send and Reply Portals
- Enable and Configure the Request File Portal
- Enable and Configure the Drop-Off Portal
- Enable Multifactor Authentication for the WTC
- GDPR Settings
- Guest Users
- Managing Workspaces in the VFS
- Privacy Reports
- Privacy Policy
- Restrict Workspaces Invitations to Specific Domains
- Terms of Service Agreement
- Transactional Workspaces
- Unicode File Transfers
- Upload Forms
- Viewing Data in DB Browser
- Workspaces Activity Report
- Workspaces Conditions
- Workspaces Invitations
- Workspaces Notifications
- Workspaces Permissions
- Workspaces-Related Variables
- Workspaces SSO Authentication
- Introduction to SAML (Web SSO) Authentication
- WTC & Workspaces User Guide

Introduction to Workspaces

Workspaces extends the secure and robust EFT file transfer platform with features that allow end users to easily share folders with existing and new user accounts, without burdening the IT administrator. Workspaces empowers end users to share folders quickly and easily, while IT administrators retain full control and visibility of the file transfer infrastructure, leveraging the highest levels of security, regulatory compliance, flexible authentication, and data encryption aspects of the EFT platform. No file sync and share vendors have the underlying security features empowered by EFT for Workspaces as a sharing solution (DMZ Gateway, multiple secure protocols, workflow automation, flexible authentication, etc.).

Administrators Retain Control

IT administrators are able to delegate to end users the power of managing shared folders with existing and new users without losing governance, visibility, and control. End users are given a tool that fulfills the workflows they have become used to (online file sharing) in a way that conforms to corporate policy. Workspaces gives IT administrators the freedom to deny access to cloud-based file sharing services within their organization, because they have provided a safe alternative to their internal customers.

When a user's folders are shared, via the Web Transfer Client, the shared folder appears in the EFT administration interface on the **VFS** tab under the **Workspace** node.

Here, the administrator can see:

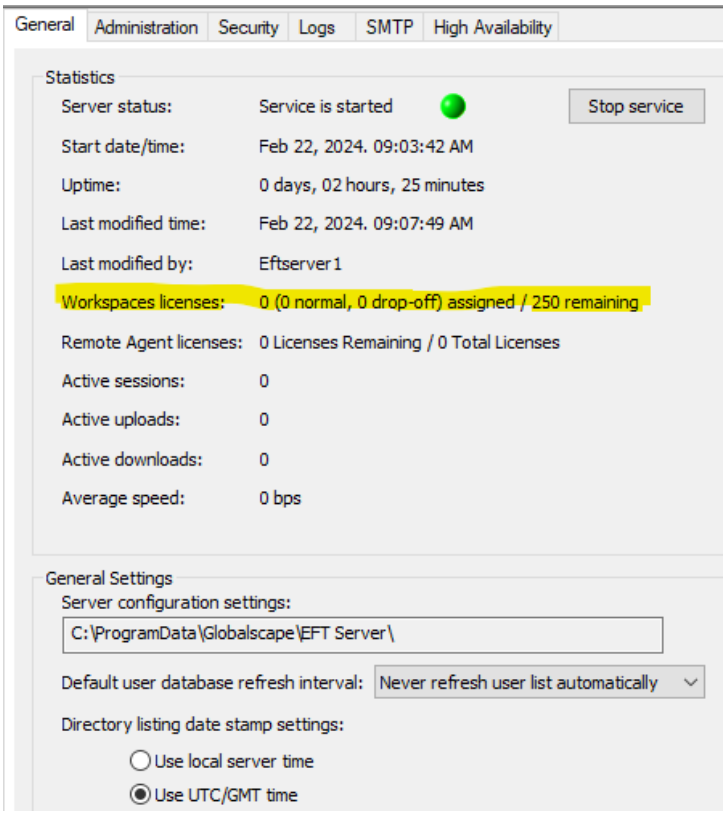
- With whom the folder is shared
- What the permissions are on each user account
- When the Workspace was created
- The physical path to the folder
- Who owns the folder

The administrator can also add or remove specific permissions on the folder for each participant.

Workspaces Licenses

In the EFT trial, you have a 100-seat license, meaning 100 users can create Workspaces. After you activate EFT, you get the number of licenses that you purchased. Activation of the HTTP/S module includes 5 Workspaces licenses.

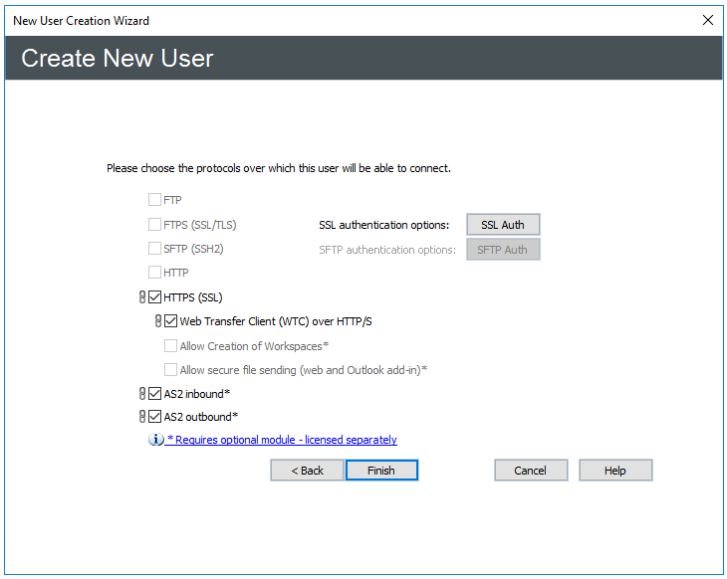
The Site's **General** tab displays how many licenses are consumed (assigned) and how many remain.



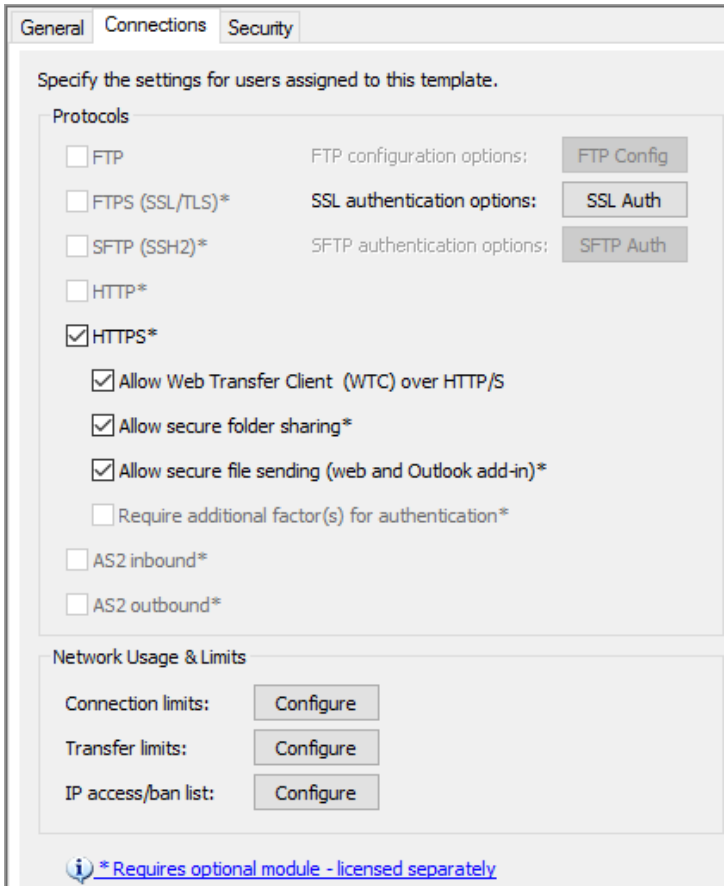
There is no limit to the number of Workspaces each Workspaces owner may possess. Licenses are applied to number of Workspaces *owners* (seats per Site), not the number of Workspaces created. (The safe operating limit is 1,000 files and folders total).

You can allow or deny Workspaces creation to specific users in the user account, settings template, and Create User wizard:

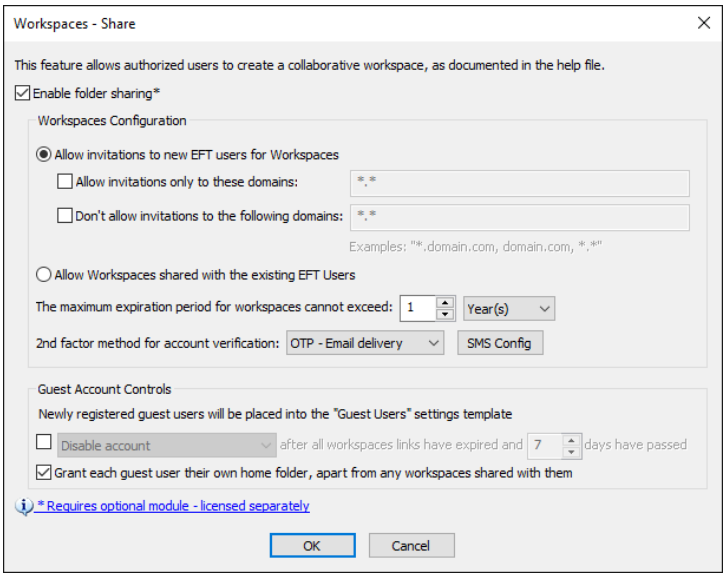
- When you create a user, select or clear the **Allow Creation of Workspaces** check box.



- In the **Site > Settings templates > Default Settings** (and other settings templates) **> Connections** tab, select or clear the **Allow secure folder sharing** check box. (Selected by default.)



- On the **Site > Web > Folder sharing** (Workspaces share) dialog box, select or clear the check box to enable folder sharing (Workspaces creation).



- Guest Users Settings Template
- Transactional Workspaces
- Sending Files with the Outlook Add-In
- Enable-Disable Send and Reply Portals

WTC Admin-Configuration Settings

The EFT administrator can configure the defaults for the WTC settings, to better control the user experience.

The **admin-configuration.json**file provides several default settings, shown below with the defaults. The default location of the file is:

C:\Program Files\Globalscape\EFT Server\Web\Shadowfax\wtc\assets

admin-configuration.json

```
{
  "batchDownloadAsZipThreshold": 5,
  "concurrentUploadLimit": 5,
  "crcEnabled": true,
  "defaultDateTimeFormat": "DD-MM-YYYY HH:MM:SS",
  "defaultLanguage": "auto",
  "defaultNumberFormat": "111,111.00",
  "defaultOpenPanel": "none",
  "displayFullName": false,
  "fileListingDisplayLimit": 500,
  "idlePeriodBeforeLogoffMS": 300000,
  "keepAlivePingMS": 200000,
  "timeoutWarningDurationMS": 20000,
  "tunnelNonHttpVerbs": false,
  "uploadChunkSize": 200000000,
  "workspaceDefaultPermissions": {
    "canCreateFolder": true,
    "canDeleteFile": true,
    "canDeleteFolder": true,
    "canDownloadFile": true,
    "canRenameFileFolder": true,
    "canUploadFile": true
  },
  "workspaceParticipantLimit": 0
}
```

These default settings can be overridden by the user's settings for time/date format, number format, language, and open panel. That is, if a user has logged in before on a particular browser, the previous preferences will take effect.

Deleting the local storage entries will allow a refresh for the administrator values to take effect. For example, while logged out of the WTC in Chrome, click **Settings** > **Privacy and Security**. Then in **Clear browsing data**select the **Cached images and files** check box, then click **Clear data**.

Enable HSTS

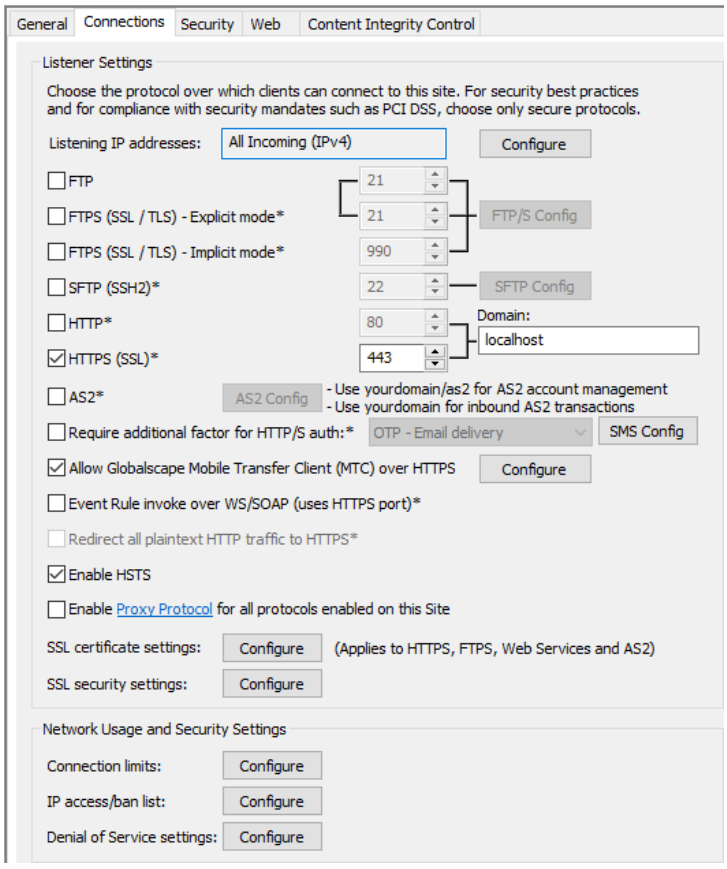
HTTP Strict Transport Security (HSTS) is web security policy to protect websites against protocol downgrade attacks and cookie highjacking. You can use HSTS response headers to tell browsers that your site only works via HTTPS. The response header indicates to the browser that you don't want to use HTTP requests, and it will automatically make requests to the same origin with a secured connection. When you try to access the same URL via HTTP again, browsers will use HTTPS and redirect internally.

- HSTS can be enabled in the administration interface without "HTTP -> HTTPS redirect" enabled.
- HSTS is available only when HTTPS is enabled.
- EFT sends HSTS headers when the client connects (if HSTS is enabled).
- HSTS is enabled by default on new installs when HTTPS is enabled.
- HSTS is enabled by default on upgrades if HTTPS was enabled before the upgrade.
- HSTS is part of the HTTP/S module.

> **NOTE:** A more granular way of defining which resources and actions are allowed on your website is to define a Content Security Policy (CSP) header. For more about CSP, refer to Knowlegebase article 11435 - Specify CSP.

To enable HSTS

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Connections**tab.



4. Select the **Enable HSTS** check box.
5. Click **Apply**to save the changes on EFT.

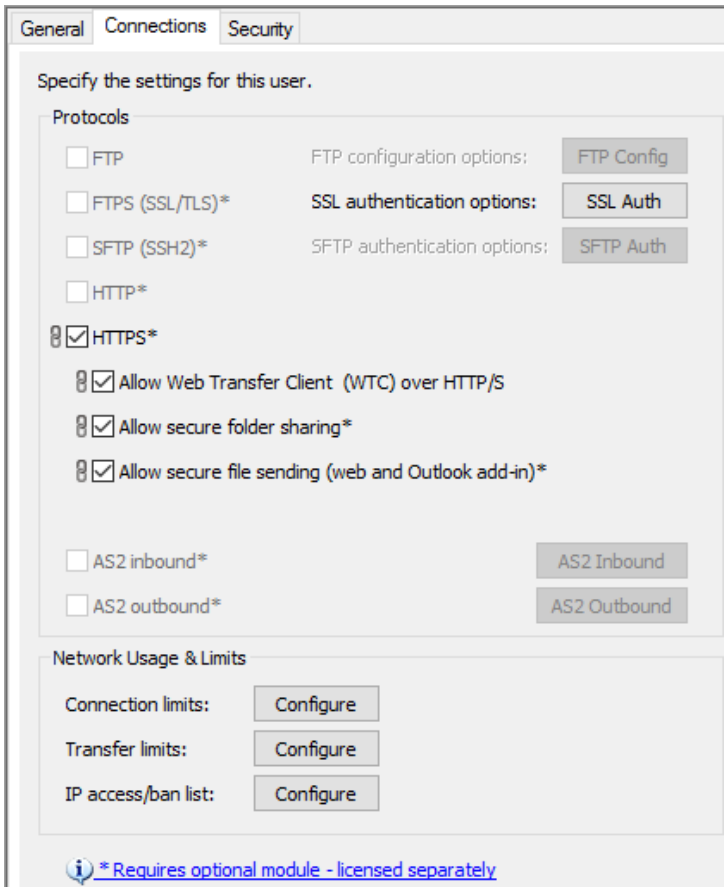
Allow Users to Create Workspaces

(Requires the HTTP/S module and Workspaces module) Users must log in to Workspaces via the Web Transfer Client (WTC). The EFT administrator must configure EFT to allow connections from the WTC. See also Enabling User Access to the Web Transfer Client and Enable and Configure EFT Workspaces.

- Active Directory domain users must have logon permission on EFT computer to log on to EFT through the WTC. This is accomplished by adding AD domain users to the "Allow log on locally" list on the EFT computer. If an AD domain user is not in this list, logging on to EFT through the WTC will fail and an error message appears informing the user that Local login access is required to log on to EFT.
- Ensure that the child folders and files in EFT's \InetPub\ (**C:\InetPub**) directory have the correct permissions, as described in Set Windows NT Permissions for EFT.
- Stopping and restarting the Site disconnects everybody who is connected; users must log back in.
- The user account that is creating the Workspace must have permissions on their home folder to create folders.

To configure EFT to allow users to create Workspaces

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Settings Template or user account.
3. In the right pane, click the **Connections**tab.



4. In the **Protocols** area, select the **Allow Creation of Workspaces** check box.

   HTTPS must also be enabled.

5. Click **Apply**.

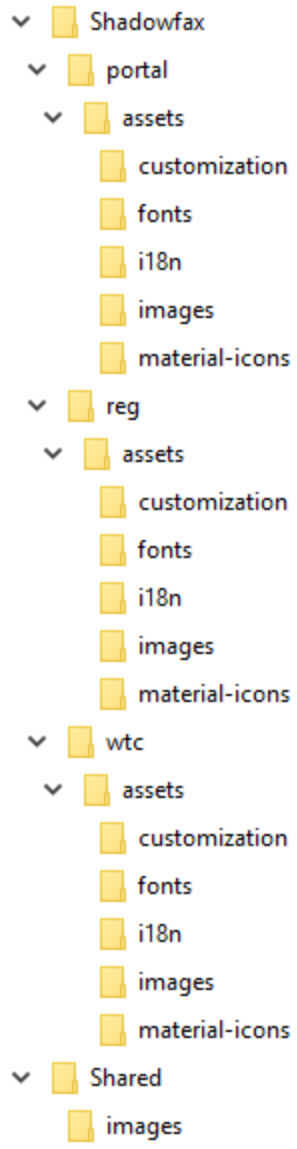
Changing Logo and Colors in the WTC and Login Page

"Rebranding" the Web Transfer Client (WTC) is a common request from customers. This topic provides the procedures for changing the logo and colors in the Login pages and in the WTC itself.

- Please make a backup copy of any files that you plan to edit, in case you have to back out your edits.
- Do not attempt to make changes to the JS or PS files unless you are well versed in doing so. In most cases, it is not necessary to change them.
- You will need to install PowerShell if you don't have it already.
- Be aware that when you upgrade from older versions to v8.0.5 or later, the file paths have changed. There is no longer an \EFTClient\ folder.

The Web folder contains shared files, reg files, WTC files, Workspaces files, and others. When changing logos, be aware of which images you need to edit. (The **\Web** directory is in the cluster share for HA installations.)

- The login page **..\Web\Account\Login.htm** uses the logo in the shared images folder
- The **forgot-username** and **lost password** pages use the logo in the **\wtc\assets\images** folder
- The **..Web\Shadowfax\portal\assets\customization** folder contains the **theme.json** file and the **customization-theme.ps1** file:
  - **theme.json** is used to define the colors used in the WTC
  - **customization-theme.ps1**is a PowerShell script used to change the colors throughout the product
- The **Shadowfax** folder contains the **portal**, **reg**, and **wtc** folders.

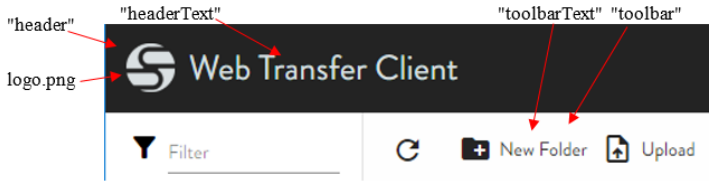


The procedures below describe how to change the colors, and then run the PowerShell script, as well as changing the logos.

The default colors in the **theme.json**file are in hexidecimal.

- "primary": "#00a8d4", - blue, used for input field outlines, e.g., the border around the password and username boxes
- "accent": "#7400d4", - purple, used for check boxes
- "warn": "#f44336", - red, used as outline for input field errors, such as invalid characters in a password
- "header": "#232323", light black background

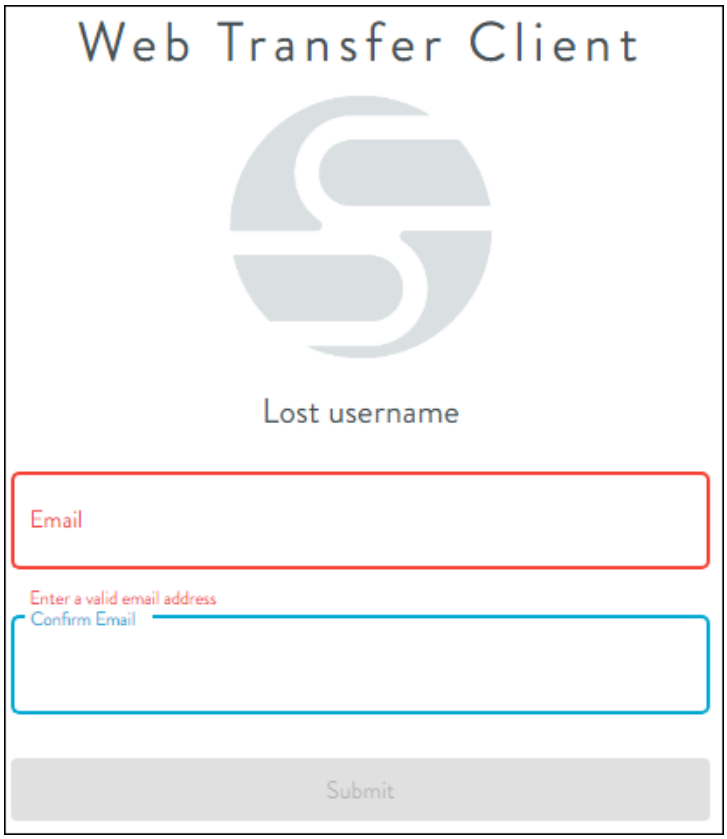
- "headerText": "#DAE0E2", the light gray text in the header, Web Transfer Client
- "toolbar": "#FEFEFE", light gray background
- "toolbarText": "#242424" light black text on the toolbar



The logo next to Web Transfer Client in the header is called **logo.png**. You can replace it with your company logo with the same file name (logo.png). The file is located in the **..\Web\Shadowfax\wtc\assets\images** folder.

To change the colors in the lost username or forgot password dialog box

1. Open **theme.json** in a text editor such as Notepad.
2. Edit the colors as desired. (You can find color numbers on the Internet or use Adobe PhotoShop to identify the color number.)
3. Save the changes to **theme.json**.
4. Open Windows PowerShell ISE (click **Start**, then **Search** to find it).
5. In PowerShell, open **customize-theme.ps1**, then click the **Run** icon.
6. Go to your WTC address, then click **Forgot Password** to open the forgot-username window. The text-entry boxes should be displayed in your new colors.



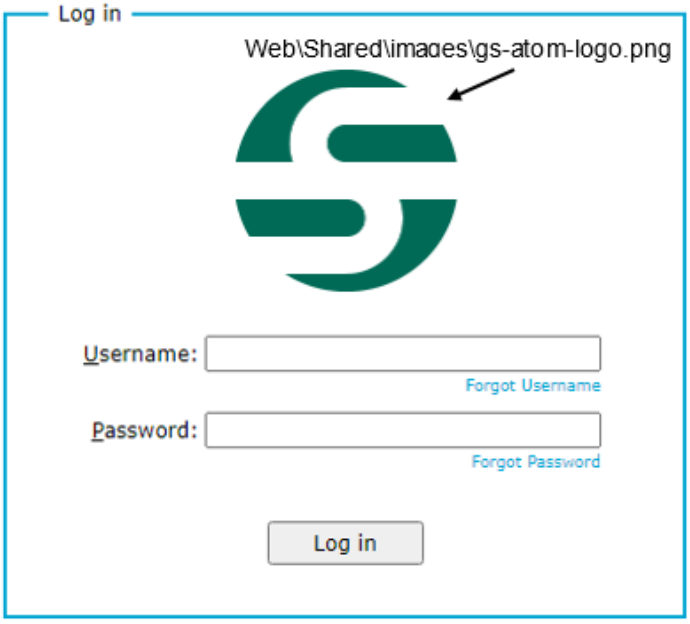
To replace the logo on the login pages

Replace the logos with your own of a similar size, then restart the Site and/or clear the browser cache to see the changes.

The WTC login page comes from EFT; the username/password logos come from Workspaces.

The logo that appears on the forgot-password page is **..\web\shadowfax\wtc\assets\images\logo.png**:

The logo that appears on the WTC login page (for example, https://localhost/Web/Account/Login.htm), the logo is **\Web\Shared\images\gs-atom-logo.png**.



For multiple sites

The procedure is basically the same, but you must first create a separate folder (as described below) for each Site that you want to customize.

1. In the **<EFT installation>\Web** folder, create a folder named **Custom** (with a capital C).
2. In the **Custom** folder, create folders named after the individual sites (e.g., MyUSsite, MyUKsite, MyCanadianSite).
3. Copy the entire **Shadowfax** folder into each of the new Site folders. For example, **..\Web\Custom\MyUSSite\Shadowfax**.
4. In each Site's **\Shadowfax\portal\assets\customization** folder (as shown above for a single site):
    a. Adjust the colors you want in the theme.json file.
    b. Run the customize-theme.ps1 script.
5. Restart the EFT Server Service.
6. View each site to verify your changes.

User Access to the Web Transfer Client

(Requires the HTTP/S module) Before users can log in to EFT using the Web Transfer Client (WTC), EFT administrator must configure EFT to allow connections from the WTC. Active Directory domain users must have logon permission on EFT computer in order to log on to EFT through the WTC. This is accomplished by adding AD domain users to the "Allow log on locally" list on EFT computer. If an AD domain user is not in this list, logging on to EFT through the WTC will fail and an error message appears informing the user that Local login access is required to log on to EFT.

Setting Defaults

The admin-configuration.jsonfile is used to set defaults for all the WTC settings, providing better control over the end-user experience, such as upload limit, permissions, participant limit, and others. The file can be opened and edited in a text editor and is stored in the ..**\Web**directory. (The **\Web** directory is in the cluster share for HA installations.)

In v8.0.4 and earlier: **Web\public\EFTClient\shadowfax\wtc\assets**

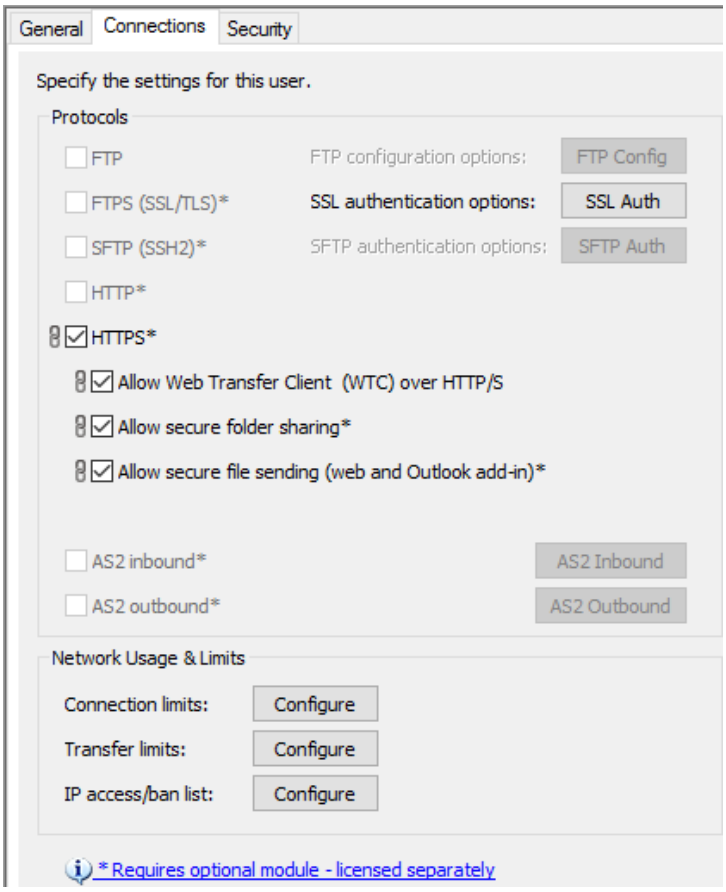
In v8.0.5 and later: **\Web\Shadowfax\portal\assets**

Refer also to Enable Multifactor Authentication for Workspaces

Stopping and restarting the Site disconnects everybody who is connected; users must log back in.

To configure EFT to allow Web Transfer Client Connections

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Settings Template or user account.
3. In the right pane, click the **Connections**tab.



4. In the **Protocols** area, select the **Allow Web Transfer Client over HTTP/S** check box.

   HTTPS must also be enabled.

5. Click **Apply**.

Folder Sharing (Workspaces)

(Requires HTTPS, Workspaces) The Workspaces feature of EFT allows end users to share their folders with other users. The user account that is sharing the folder maintains control of permissions to the shared folder, and can revoke sharing privileges at any time. Workspaces provides the ability to easily share and collaborate on information that is securely managed by EFT, including existing authentication, access control, auditing, governance, and Event Rule workflow capabilities available in EFT.

If an unsigned or otherwise invalid certificate is used in the Chrome browser, downloads will fail, even if you add the certificate to your trusted list. To resolve this issue, use a valid, signed certificate. Alternatives include:

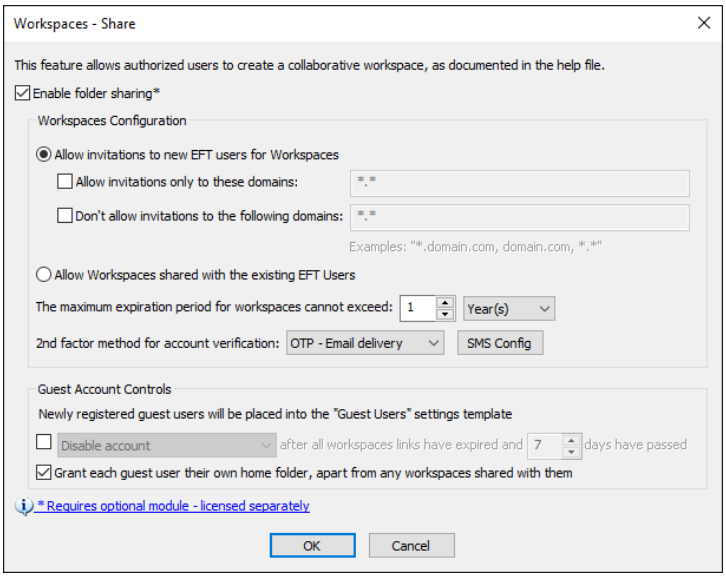
- Use a different browser
- Block downloads until you get a valid certificate
- Create a self-signed certificate outside of EFT, use a subject alternative name (SAN), then add the certificate to Chrome's trusted list.

Refer to Workspaces Licensesfor important information regarding Guest Accounts.

To enable Workspaces on the Site

(Refer to To enable Workspaces for a Settings Template or specific users below to disable/enable Workspaces for specific Settings Templates or users.)

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the Webtab.
4. Next to **Folder sharing**, click **Configure**. The **Workspaces - Share** dialog box appears.



5. Select the **Enable folder sharing** check box.
6. Under **Workspaces Configuration**, specify one of the following groups of users (any users or only existing EFT users) to whom users can send Workspaces invitations:
    - **Allow invitations to new EFT users for Workspaces**
        - (Optional) Select the**Allow invitations to these domains** check box, then specify the domains to which Workspaces users can send invitations, comma/semicolon delimited. Wildcards are supported (for example, *.domain.com or domain.com). The setting is not selected by default; that is, all domains *.* are allowed. (**Allow invitations to new EFT users for Workspaces** must be selected.) NOTE: Be sure wildcards are formatted correctly. That is, if you specify *.domain.com, then the domain www.domain.com is allowed.
        - (Optional) Select the **Don't allow invitations to the following domains** check box, then specify the domains for which you do not want to allow access to Workspaces. The field is comma/semicolon delimited; wildcards are supported (for example, *.domain.com or domain.com). The setting is not selected by default; that is, no domains *.* are blocked. NOTE: Be sure wildcards are formatted correctly. That is, if you specify *.domain.com, then the domain www.domain.com is blocked.
    - **Allow Workspaces shared with existing EFT users**
        - On an LDAP-authenticated Site, when a sender types a recipient email to share a Workspace, if that email does not belong to a local

(cached) account in EFT, EFT will extend its search to the LDAP authentication database.

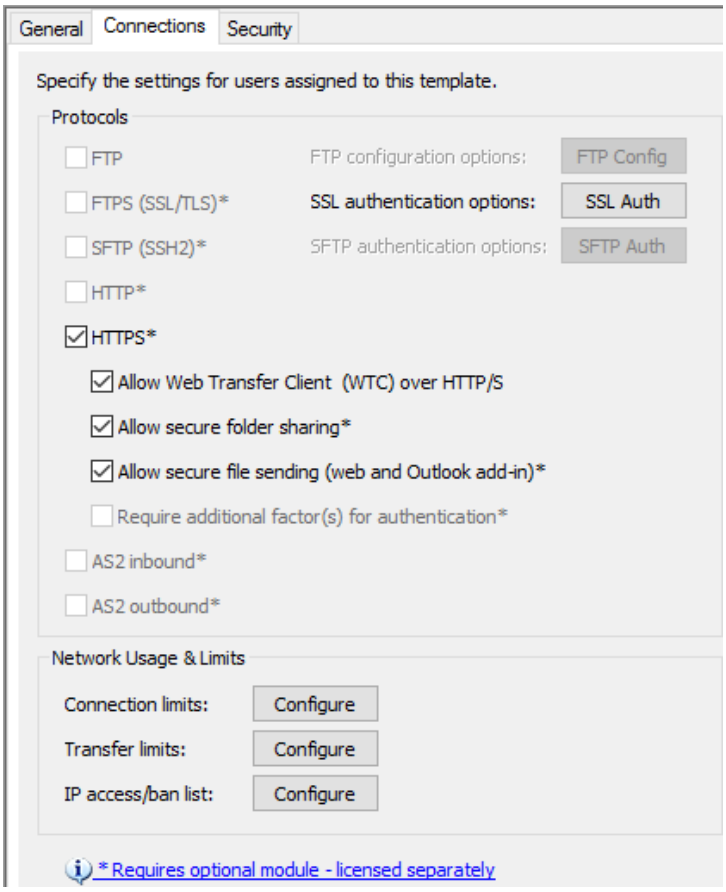
- Specify the **maximum expiration period** for a Workspace. Senders can set the expiration to happen sooner than what is defined on the server, but you cannot specify a longer period. (Refer to Enable Send Portal for information about retaining files after a Workspace link has expired.)
- Specify **2nd factor method** for account verification (OTP) options. Refer to Enable Multifactor Authenticationfor directions.

7. Under **Guest Account Controls**:
   - Specify whether to **Disable account**, **Remove account and home folder**, or **Remove account only**after all Workspaces links have expired and *n*days have passed. When set to 0 days, the account(s) will be cleaned up at midnight. If the Guest account is disabled, the user will not be able to log in unless the EFT administrator enables or removes the account (and then the guest user would have to recreate their account). Refer to Workspaces Invitations for an example of using the **User Account** action to enable an expired Guest account.
   - To grant guest users their own home folder, select the **Grant each guest user their own folder** check box. Selecting the check box prevents guests from viewing other files in the Workspace's home folder.

     If the check box is ***not***selected, the user has:
     - Read-only access to home folder.
     - List view of Workspaces with permissions as allowed by Workspaces owner, regardless of any protocols used to access the account.
8. Click **Apply**to save the settings.

To enable Workspaces for a Settings Template or specific users

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Settings Template or user account.
3. In the right pane, click the **Connections**tab.



4. In the **Protocols** area, select the **Allow secure folder sharing**check box. If this check box is not available, you have not activated the Workspaces licenses or the trial has expired; or you have not enabled Workspaces for the Site.

   HTTPS must also be enabled.

5. To also allow secure file sending in the WTC and in the Outlook add-in, ensure that the **Allow secure file sending** check box is selected.
6. (Optional) To enable additional authentication by email or SMS, select the **Require additional factor(s) for authentication** check box.
7. Click **Apply**.

Related Topics

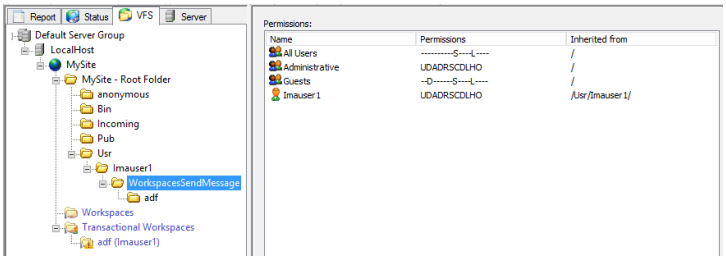
- Enable Multifactor Authentication for the WTC
- Workspaces SSO Authentication
- Guest Users
- Workspaces
- Sharing Folders

- Workspaces Activity Report
- Workspaces for Outlook

Send and Reply Portals

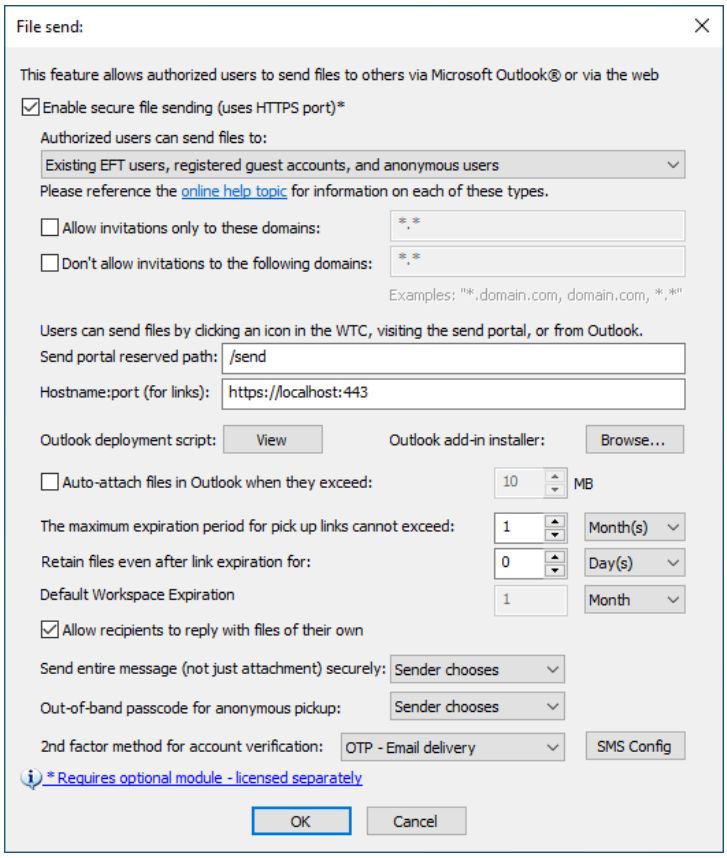
(Requires HTTPS, Workspaces) Workspaces is an enterprise ad hoc file transfer solution that allows employees to quickly and securely send large files from within the Web Transfer client or in Microsoft Outlook. Workspaces for Outlook allows organizations to address broad scale, risky file sharing practices while providing an easy-to-use interface for end users that requires little to no training from IT staff. Users benefit from an enhanced email experience with advance sending features, such as the ability to receive file pick up receipts. Recipients pickup their files in their web browser via a secure link. Administrators have the ability to manage user transactions behind the scenes, including the ability to set secure link expiration overrides and set policies for the automatic handling of exceedingly large file attachments.

- **MFA in the WTC** is disabled by default. Refer to Enable Multifactor Authentication for the WTC for instructions for enabling it.
- **MFA in Workspaces** is enabled by default. Refer to the procedure below for instructions for configuring it.
- To use Workspaces for Outlook, the EFT administrator must enable Workspaces and install and enable the EFT Outlook Add-In on end-users' computers, as described below.
- On the user account, the **Allow secure file sending**check box must be selected.
- When you send a file in the Web Transfer Client, a **WorkspacesSendMessage** folder is created under the sending user's home folder in the Virtual File System (VFS). Subfolders in the **WorkspacesSendMessage**folder are named for the Subject line of the message.



To enable Workspaces for sending files

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Web**tab.
4. Next to **Send Portal,**click **Configure**. The **File send** dialog box appears.



5. Select the **Enable secure file sending** check box. This requires the HTTPS port to be configured and available.
6. Under **Authorizedusers can send files to**, select one of the following options:
    - **Existing EFT users only (most restrictive)** - Allows EFT users to send files via Workspaces for Outlook only to other users with an EFT account
    - **Existing EFT user and registered guest accounts** - Allows EFT users to send files via Workspaces for Outlook to other EFT user accounts and registered guest accounts
    - **Existing EFT users, registered guest accounts, and anonymous users** - Allows EFT users to send files via Workspaces for Outlook to other EFT user accounts, registered guest accounts, and non-EFT user accounts. Non-EFT user accounts do not require credentials, making it easy for the recipient to pick up files, but makes the system less secure. To reduce this risk, the sender can make the pickup link "single use."

      Transactional Workspacesfolders in the VFS that are shared with unregistered users will have an exclamation point on the anonymous-access folder.

7. To limit sending invitations to certain domains, select the **Allow invitations only to these domains** check box, then specify the domains, separated by commas.
8. To prevent sending invitations to certain domains, select the **Don't allow invitations to the following domains**, then specify the domains, separated by commas.

   In the **Send portal reserved path** box, specify the path for the **Send**portal. The default is **/send**.
9. In the **Hostname:port**box, specify the URL for file pick up. By default, this box will contain the same IP as the Domain box on the **Site > Connections** tab, but you can change it to an external-facing hostname, if needed (and if so configured in your network). Links that are sent for Workspaces invitations and file sharing will have this URL.
10. For using the Outlook deployment script or Add-In installer, refer to Deploy Outlook Add-In on End-User's Computers.
11. To require the use of Outlook for large files, select the **Auto-attach files in Outlook when they exceed** check box, and then specify a size.
12. Specify the **maximum expiration period for pickup links**. The default is 1 month.

13. Specify the length of time to **Retain files after link expiration**. The default is 0 days.
14. This value indicates the length of time between Workspace expiration and file removal, and cannot exceed **maximum expiration period**, above. On expiration, a "Workspace expired" Event is triggered and the Workspace becomes invisible to the administrator, owner, and participants, but the directory and files remain alive. At the end of the retention period, a "Workspace removed" Event is triggered, the Workspace information is wiped from EFT configuration, and the directory is physically removed from the file system. For example, if a transactional (guest user) Workspace is created to expire in 10 days and retain file for 10 days, if the Workspace expired on October 1, it will then be removed from disk on October 11.
15. Specify a **Default Workspace expiration** time as 1 day, week, month, year, or immediately. The value defined here is inherited for all Workspace users for Send/Request/Outlook add-in, and listed as the default **Message Expiration** under **Options** in the WTC and under **Default Send Options** in the Outlook add-in. The default value is 1 Month.
16. Select the **Allow recipients to reply with files of their own** check box to allow people that you send file to reply with files of their own. Then you must enable the Request file page to specify the **Reply** path.

    After a recipient has received a message sent through Workspaces, the recipient can reply to the email in the Workspaces Reply Portal (if so configured) and send files back to the sender. If you do not want to allow that functionality, you can disable replies. Disabling the Reply portal removes the request files functionality from the Web Transfer Client interface.

17. Next to **Send entire message (not just attachment) securely**, click the **Sender chooses** drop-down list and click an option:
    - **Always secure** - Always send message and attachment securely
    - **Never secure** - Never send message and attachment securely
    - **Sender chooses** - Sender can choose whether to send message and attachment securely

18. **For anonymous recipients**: Next to **Out-of-band passcode for anonymous pick up**, specify whether a recipient requires a passcode to pick up files. Click the drop-down list and then click **Required** (sender must require a passcode), **Not required**(sender does not have to require a passcode), or **Sender chooses** (whether to require a passcode). (The sender's authentication options appear in the **Options**dialog in Workspaces.) When an out-of-band passcode is required, the passcode will appear for the sender after the message is sent. The sender then must provide the recipient the passcode via a non-Workspaces method (for example, phone, email, SMS, or message app).
19. Next to **2nd factor method for account verification**, click the list to choose one of the methods of delivery for the OTP:
    - **OTP - Email delivery** - EFT does not verify SMTP server configuration
    - **OTP - SMS delivery** - If no mobile number is available for the user, SMS delivery will fail.
    - **OTP - try SMS then Email** - EFT first looks for mobile number in the user details. If no mobile number is defined, the email address is used.
20. Click **SMS Config** to configure SMS options, such as Twilio. Refer to Enable Multifactor Authentication for details.
21. Click **OK**, then click **Apply** on the **Web** tab.

Related Topics

- Installing the EFT Outlook Add-In
- Deploy Outlook Add-In on End-User's Computers
- Using EFT Outlook Add-In

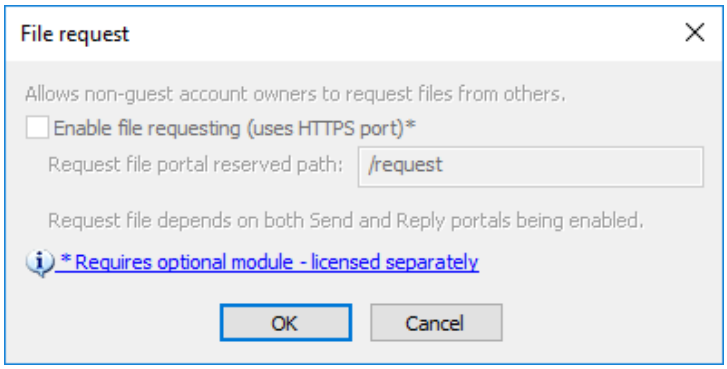
Request File Portal

(Requires HTTPS, Workspaces) After you enable the Send and Reply portals, then you can enable the **Request file** portal and specify the **Request file portal reserved path**as described in the procedure below.

The Request file portal requires that the HTTPS port is enabled, as well as both the Send and Reply portals. (Select the **Allow recipients to reply with files of their own** check box in the **File Send** dialog box.)

To enable the Request file portal

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Web**tab.
4. Next to **Request file portal,** click **Configure**. The **File request** dialog box appears.



5. Select the **Enable file requesting** check box, then specify the reserved path.
6. Click **OK**.

Related Topics

- Configuring HTTP or HTTPS Transfers
- Enable and Configure EFT Workspaces
- Enable Send and Reply Portals

Drop-Off Portal

(Requires HTTPS, Workspaces) The Workspaces Drop-Off portal allows employees and partners to send files to internal users, with no attachment limits. The transfer of the email and attachments is encrypted and secure. The Drop-Off portal is configured at the Site level on the **Web** tab.

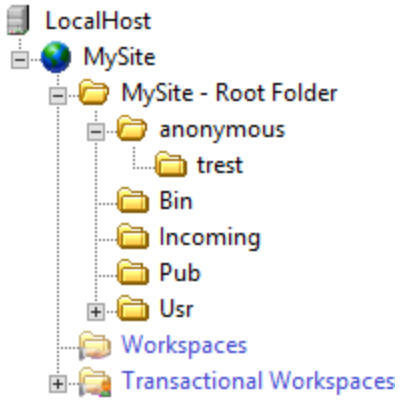
A Workspaces license is consumed for each Drop-off portal message no matter how many recipients the message has.

A Workspaces license is **not**consumed on replies.

A Workspaces license is **not**consumed on Send Portal messages.

You can avoid Workspaces licenses being consumed by the Drop-off portal by disabling the Drop-off portal. It is not enabled by default.

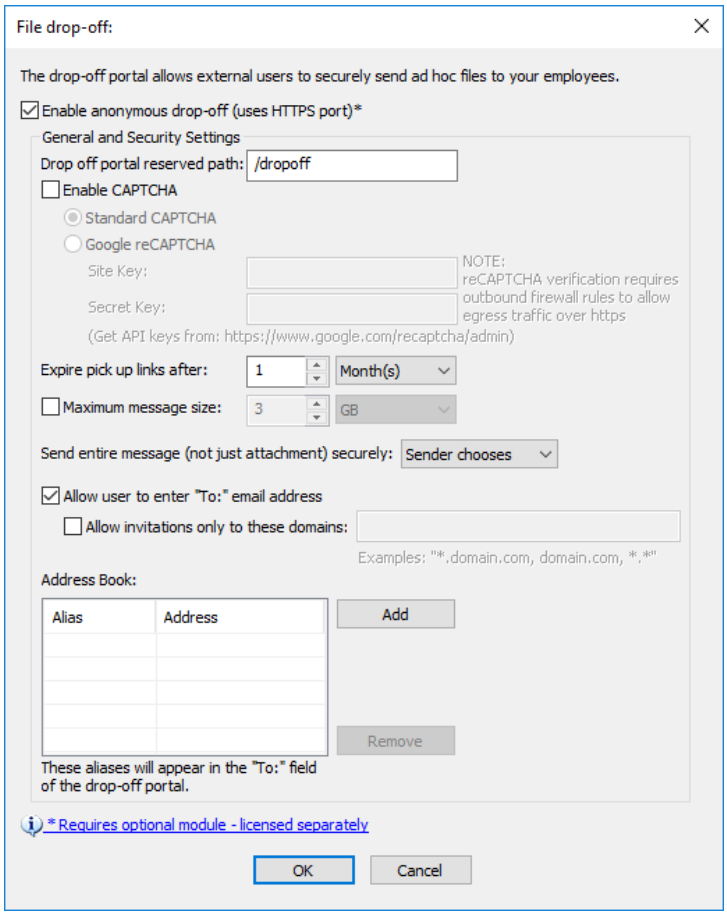
When someone uses the drop-off portal, that "someone" becomes a "Workspaces owner." This is because behind the scenes, a temporary, anonymous account is created to host the Workspace, thus consuming a license (assigned to that account). A folder, named with the Subject line of the email, appears under the **anonymous**folder in the VFS. Once the Workspace expires, the anonymous account is also removed, and the license is released to the pool.



- For additional security, you can configure Google's reCAPTCHA on the Site, as described below.
- You will need to add Google's domain to the Content-Security-Policy (CSP) header for reCAPTCHA to work. Refer to https://kb.globalscape.com/KnowledgebaseArticle11435.aspxfor details.
- Instruct Workspaces users that they must complete the CAPTCHA ***before***they attempt to attach files to the portal. Otherwise, the files won't attach.

To enable the Drop-Off portal

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. On the **Web**tab, next to **Drop-Off portal**, click **Configure**. The **File drop off** dialog box appears.



4. Select the **Enable anonymous drop-off** check box. This requires the HTTPS port to be configured and available.
5. Specify a portal reserved path if you want something different from the default (/dropoff). The hostname:port are configured in the File Send dialog box.
6. (Optional) To use captcha, select the **Enable CAPTCHA**check box.
    a. Specify whether to use **Standard CAPTCHA** or **Google reCAPTCHA**. reCATCHA verification requires outbound firewall rules to allow egress traffic over HTTPS.
    b. If you click **Google reCAPTCHA**, refer to the reCAPTCHA procedure below, then specify the following keys:

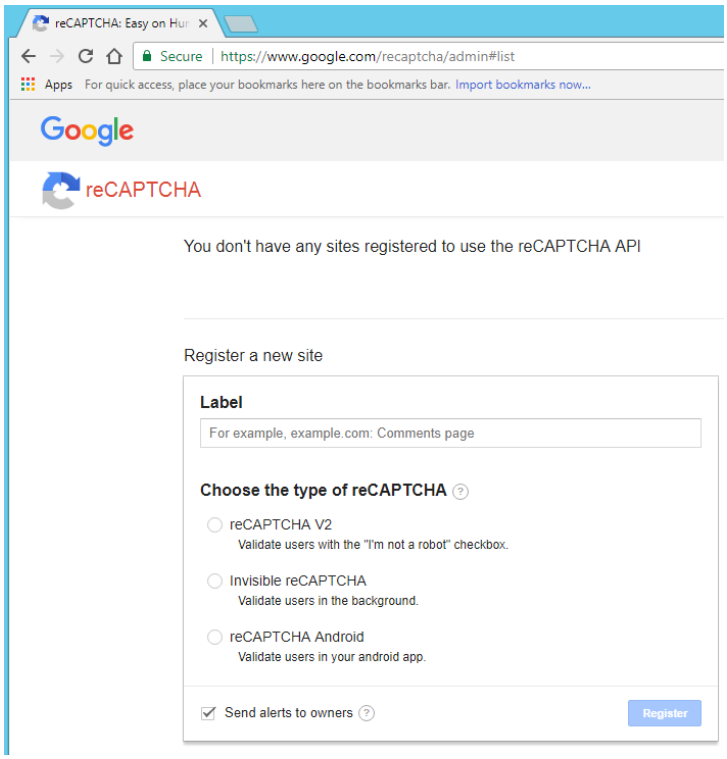
- In the **Site Key** box, paste the Google Site Key.
- In the **Secret Key** box, paste the Google Secret Key.

If the Drop-Off portal is enabled, and Google reCAPTCHA is enabled, a prompt appears. You will need to add Google's domain(s) to the Content-Security-Policy (CSP) header for reCAPTCHA to work. Refer to https://kb.globalscape.com/KnowledgebaseArticle11435.aspxin the Globalscape Knowledgebase for instructions.

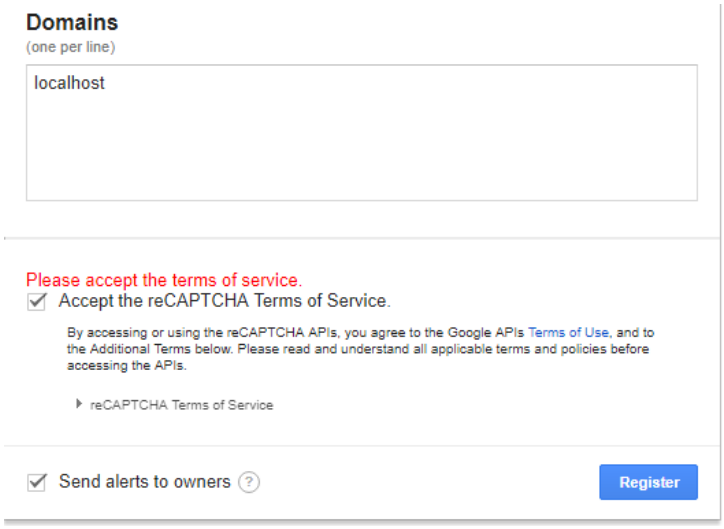
7. In the **Expire pick-up links after** boxes, specify the number of **Days**, **Weeks**, **Months**, or **Years** before a pick-up link expires. Be aware that using the Drop-Off portal consumes a Workspaces license, which is not released until the link expires. The default expiration is 1 month.
8. (Optional) Specify the **Maximum message size**. If the **Maximum message size** check box is not selected, the maximum message size is 3 GB. Knowledgebase article #11389describes an advanced property that you can use to set the maximum anonymous uploads size in GB. If the **MaxAnonymousAllUploadsSizeInGB**advance property is set to a value that is LESS than **Maximum message size** in the **File drop-off**dialog box, an error occurs stating that the file is too large.
9. Specify the **Secure the message body** setting: **Always secure**, **Never secure**, or **User Choice**. **User Choice** is the default.
10. (Optional) Specify whether to allow users to enter a **To** email address.
    - If you are allowing users to enter a To email address, specify which domains are allowed (for example, *.mycompany.com, *.mypartner.com). If you leave the box blank, you have an "open-relay" server, which is not recommended. Suggested domains include your organizational domain(s) and other necessary domains.
11. In the **Address Book**, add one or more addresses and aliases that will appear in the **To** field.
    - The **Alias**that you define in the address book will appear in the To box in the Drop-Off portal. Having the alias avoids leaving the complete email address exposed. This is useful in cases such as if you are mailing a PDF form to multiple clients who might not want you to share their email address with everyone.
12. Click **OK**, then click apply on the **Web**tab.

To configure reCAPTCHA for the Drop-Off portal

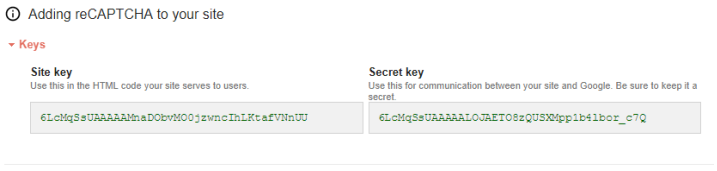
1. If you want to enable CAPTCHA, before you enable and configure the Drop-Off portal, go to https://www.google.com/recaptcha/administratorand log in to your Google account.



2. Click **reCAPTCHA v2**. The **Domains** box appears.



3. In the **Domains**box, type one or domains (Sites) that are to use reCAPTCHA.
4. Select the **Terms of Service** check box.
5. Click **Register**. The keys appear.



6. Save the Site key and Secret key. You will need these to configure the Drop-Off portal in EFT if you are enabling CAPTCHA.

Related Topics

- Enable and Configure EFT Workspaces
- Enabling Workspaces to Send Files
- Workspaces Invitations
- Use the Drop-Off Portal
- Licensing Workspaces

Multifactor Authentication for the WTC and Workspaces

Multifactor authentication is the process of verifying the identity of a user in which the user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

Two-factor authentication (2FA), a subset of multi-factor authentication, is a method of confirming users' identities by using a combination of different factors: 1) something they know, 2) something they have, or 3) something they are. A common example of 2FA is withdrawing money from an ATM: only the correct combination of a bank card (something the user possesses) and a PIN (something the user knows) allows the transaction to be carried out.

EFT offers multi-factor authentication (MFA) for recipients in the Pickup portal, with which a time-based one-time passcode (OTP) is delivered automatically to the recipient's email address or via text message. When attempting authentication, the account is locked out for 5 minutes after 5 failed attempts in a 5-minute period. If the first attempt fails, a user can repeat registration and get a new verification code after 5 minutes have passed since the previous registration attempt.

Refer to Enable and Configure the Send Portal for MFA settings in Workspaces.

> **NOTE:** 2FA does not apply to the following situations: Anonymous TWS (authentication is not required for those messages), protocols other than HTTP/S, and EFT managed clients (MTC, RAM, Outlook Add-In). The Outlook Add-In does not require the Advanced Property "UserAgentHeaderMustUseOTP" to be entered since we allow the OAI to work by default.

How does MFA work in EFT?

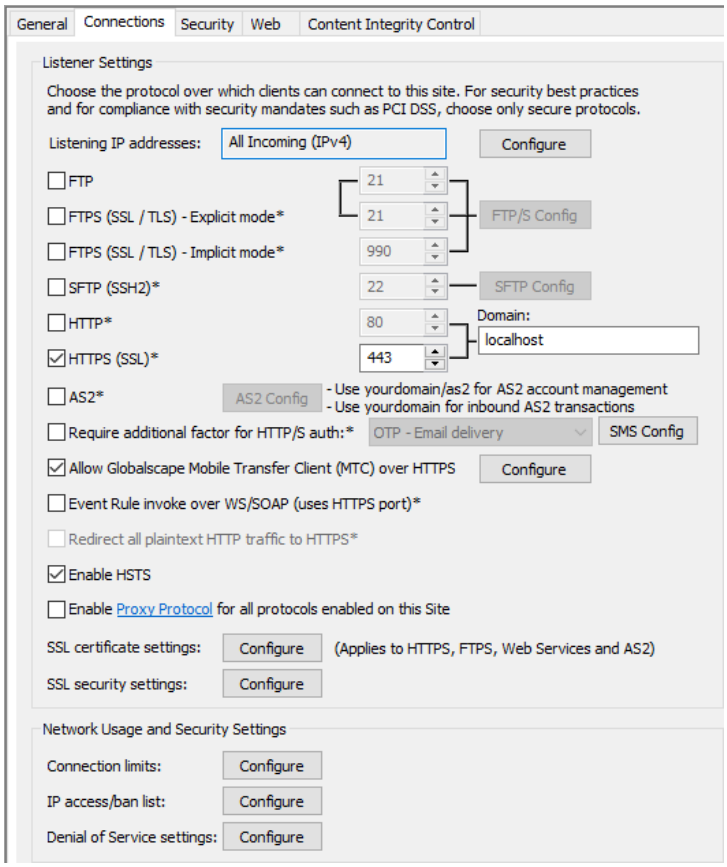
1. When logging in to the WTC, if the **Require additional factor for HTTPS auth** check box is selected and configured (shown below), the WTC prompts for a passcode, and informs the recipient to check their email or text messages.
2. EFT generates a OTP and sends it in an email or text message to the recipient. (The user account details must include their mobile phone number to use SMS; otherwise the email address is used. Therefore, for ad hoc interactions, you should specify email delivery of the OTP.)
3. The recipient checks email/text, and copies the passcode to the clipboard (or clicks the link).
4. The recipient pastes the passcode (or follows link) in the WTC.
5. If the passcode is verified, the WTC allows access.

> **NOTE:** Be sure each account has an email address specified so that no one is locked out of their account when MFA is enabled. Otherwise, EFT will not be able to email the passcode to log in.

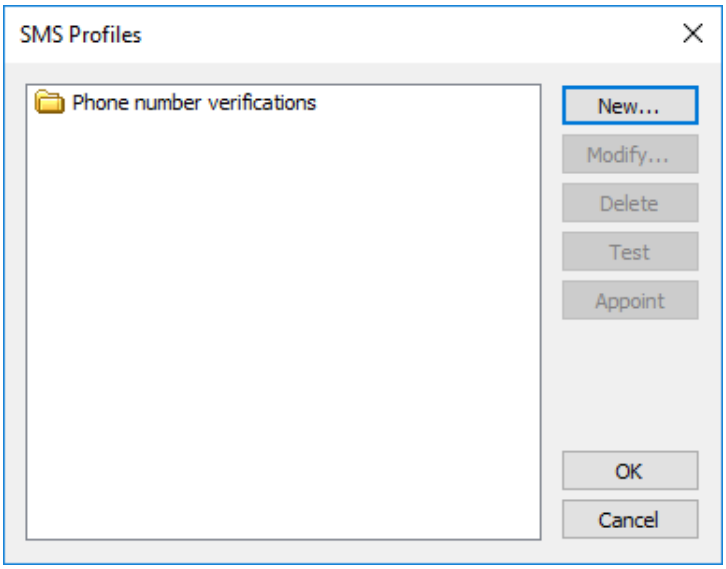
To enable and configure MFA

For SMS to work, you must first define an SMS profile on the **Site > Connections** tab. To enable MFA in Workspaces, refer to Enable and Configure Folder Sharing (Workspaces).

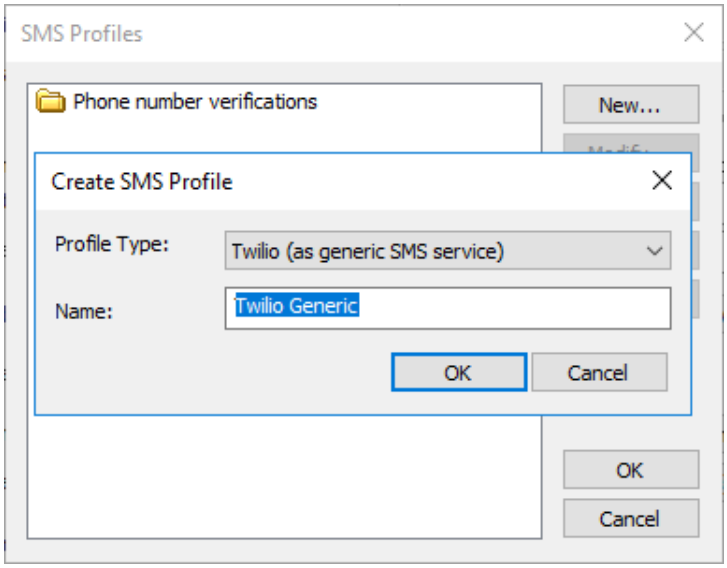
1. On the **Site > Connections**tab, enable and configure HTTPS, if not already done. (The MFA settings are inherited from the Site level, but you can enable or disable it on the Settings Template level also. You cannot enable/disable MFA at the user level.)
2. Select the **Require additional factor for HTTPS auth** check box. EFT does a quick scan of all users under that Site or Template, and if one or more users is found without an email address or mobile phone number defined, a prompt is displayed.



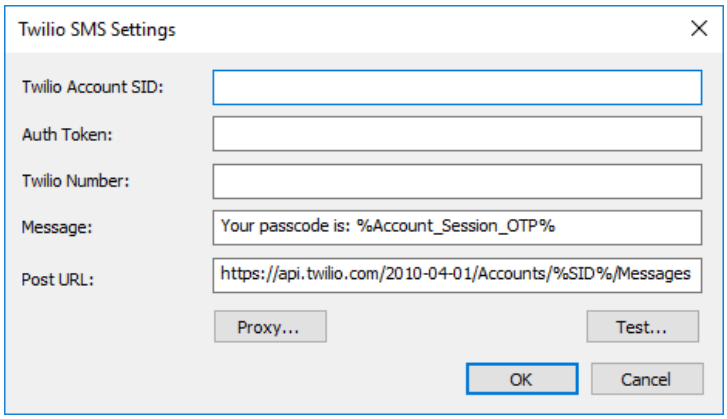
3. Click the OTP drop-down list. In the **OTP**list, select the method of delivery:
   - **OTP - Email delivery**- EFT does not verify whether SMTP server configuration is completed correctly
   - **OTP - SMS delivery**- If no mobile number is available for the user, SMS delivery will fail.
   - **OTP - Try SMS then Email**- EFT first looks for mobile number in the user details. If no mobile number is defined, the email address is used.
4. To configure the Twilio for your SMS provider, use the settings provided when you set up your Twilio account. Click **SMS Config**. The **SMS Profiles**dialog box appears:



5. **New** - Opens the **Create SMS Profile** dialog box:
    - Click **New** to create a new SMS profile (as a generic SMS or with a custom verification code).

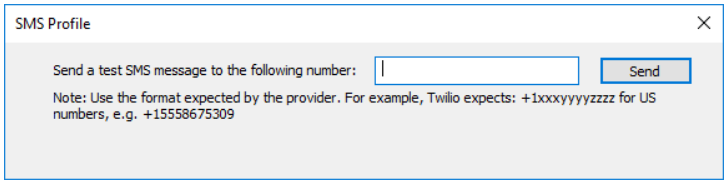


6. **Modify** - Opens the **Twilio SMS Settings** dialog box for a selected profile



   a. Provide the **Twilio Account SID** copied from your Twilio account.
   b. Provide the **Auth Token** copied from your Twilio account.
   c. Provide the **Twilio Number** copied from your Twilio account. You must include the country code and the + PLUS SIGN (that is, in the USA, +1) in front of the number.
   d. Provide the **Message**that will be sent in the SMS, but keep the variable `%Account_Session_OTP%`. This variable is used by EFT to send the OTP. Do not edit anything between the percent symbols.
   e. Provide the **Post URL** copied from your Twilio account.
   f. Configure a **Proxy**, if needed. Refer to Defining a Proxy for details.
   g. Click **Test** to verify the connection.
   h. If the test is successful, click **OK**, then click **Apply** to save the configuration.

7. **Delete** - Deletes a selected profile
8. **Test** - Allows you to send a test SMS message using the selected profile



9. **Appoint** - Assigns the selected profile to the Site.
10. On the **Server > General Tab**, edit the **Authentication OTP message**, if needed.

Important notes to consider

Multifactor activation is only applicable where account registration is required, and thus is not applicable to:

- Drop-off portal (no account is registered)
- Reply portal (you cannot reply unless you first pickup, which does require registration)
- Anonymous interactions (no account is registered)

EFT skips 2FA for following user agents:

- Anonymous ad hoc transfers (Send passcode via other means.)
- Protocols other than HTTP/S
- GlobalSCAPE-EFTApplet
- JFileUpload
- MSFT File Transfer Tool
- EFT-Mobile-Client
- Desktop Transfer Client
- GlobalSCAPE-scClient
- EFT-Outlook-Addin
- Load Balancer Agent
- ELB-HealthChecker/
- EFT Remote Agent
- When certain user-agents are defined.

If MFA is enabled, then that additional factor (OTP) will be required and enforced by EFT. The exception to this rule is when the user-agent header is on EFT's list of special agent-headers (RAM agents, MTC, CuteFTP/9, OAI, etc.).

- In addition, an advanced property override (**UserAgentHeaderSkipOTP**) is available so that administrators can add additional headers to the list, which would allow for non-Globalscape controlled clients (such as Fiddler, FileZilla, etc.) to connect over HTTPS but skip 2FA/MFA. If not defined in the advanced property exclusion list or hard-coded exclusion list, then regardless of header, the additional factor will be required to complete authentication. For example:

For CuteFTP v9.3 or later, you could use the following advanced property to whitelist the user agent and connect successfully:

```
"UserAgentHeaderSkipOTP":"CuteFTP/9.3"
```

To skip the OTP for the Edge browser when OTP is enabled.

```
"UserAgentHeaderSkipOTP":"Edge/18.18363"
```

- If the OTP provided is incorrect, EFT will retry a few more times over a short period. If after all permitted retries have been exhausted, EFT will fail registration/verification, and the account will not be created nor associated with the Workspace, and all data will be discarded. (During the time when an “unverified” user is trying but failing to complete their verification, a “valid” user can still complete the registration/verification process.)

Enabling the Account Management Page

EFT provides an HTTPS account management page on which users can reset their password, if so configured in the administration interface.

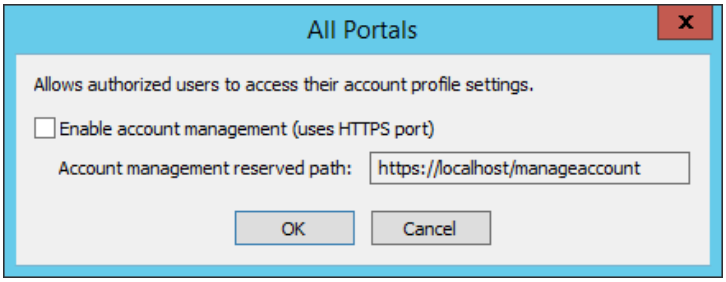
The account management page is hard-coded to https://<server-URL>**/manageaccount** with the default port of 443. If the HTTPS port is set to a different port, the user must provide the port number in the URL to log into the page (for example, **https://192.168.123.456/manageaccount:4433**).

It is ***strongly***recommended that you enable the account management page over HTTPS (using the procedure below) so that your users will be able to change their passwords. You must also enable HTTPS and SSLto use the account management page.

> **NOTE:** The account management page is not available when CAC is enabled.

To enable the account management page

1. In the EFT administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the **Site** that you want to configure.
3. In the right pane, click the Web tab.
4. Next to **Account management**, click **Configure**. The **All Portals** dialog box appears.



5. Select the **Enable account management page over HTTPS** check box. The **Account management reserve path** URL is displayed in the text box (for example, **https://localhost/manageaccount**). The URL is not editable, but you can select and copy it to provide to users.
6. Click **Apply**to save the changes on EFT.

When a user goes to the **https://<host>/managementaccount** page, they will be directed to the Web account login page, **//<host>/Web/Account/Login.htm**, and then the account management page appears. If the user is allowed to change their password, then the **Change Password for <user>** page appears. Otherwise, a message

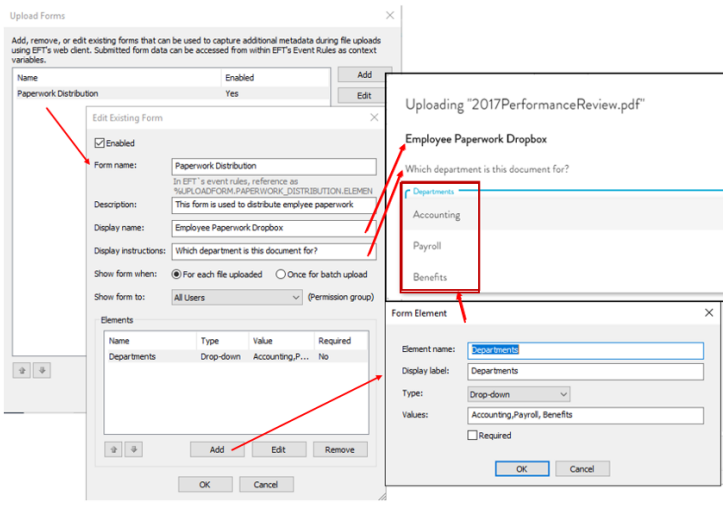
appears that says the user does not have permission to change their password. This permission is enabled on the **Security** tab of the Site, Settings Template, and User account.

Upload Forms (Secure Forms)

(Requires SFM) Upload forms are custom web forms you can create to capture metadata during file uploads when using the web client. Metadata gathered by the upload form can be used in downstream event rules (that is, subsequent Actions) for conditional post processing.

How does it work? Upon initiating an upload of a file or batch of files, and if configured to do so, EFT will prompt the end user to complete one or more forms that you created. Upon completing and submitting the form, the web client will complete the upload. EFT administrators can now access and use the form data within EFT event rules as you would any other context variables. If required fields aren't completed or the user declines the form, the upload is aborted.

When would I use upload forms?Suppose you have an electronic drop box that collects files from employees that need to be routed to the correct department: Accounting, Payroll, and Benefits. With Upload forms, you could create a form that includes a drop-down list with values for Accounting, Payroll, and Benefits, as shown in the illustration below.



In EFT's **File Upload** event rule, you would conditionally disposition uploaded documents to the appropriate department (or perform other, department-specific operations) by adding the "If %Context_Variable% does equal to string" conditional statement. The name of the upload form context variable is a combination of "uploadform" followed by the form name and element name, in the following format: `%Uploadform.Form_name.Element_name%.`

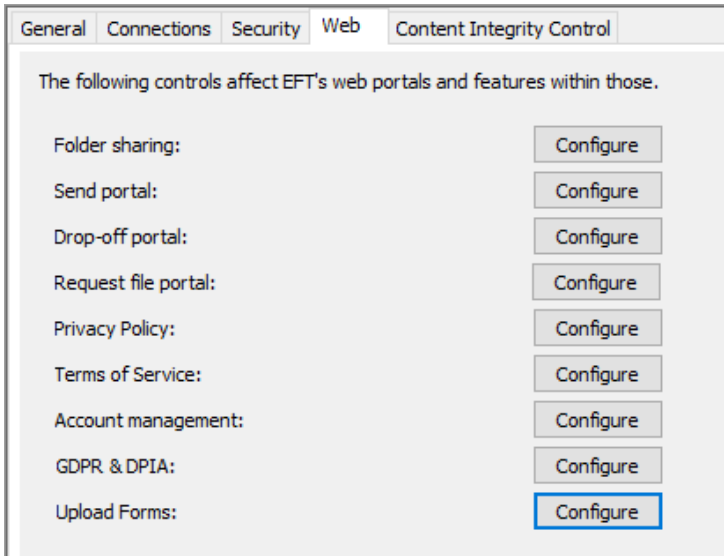
In the example above, the context variable that references the Departments values would be:
`%uploadform.Paperwork_Distribution.Departments%.`

(If you have spaces in the Form name or Element name, replace the spaces with underscores.)

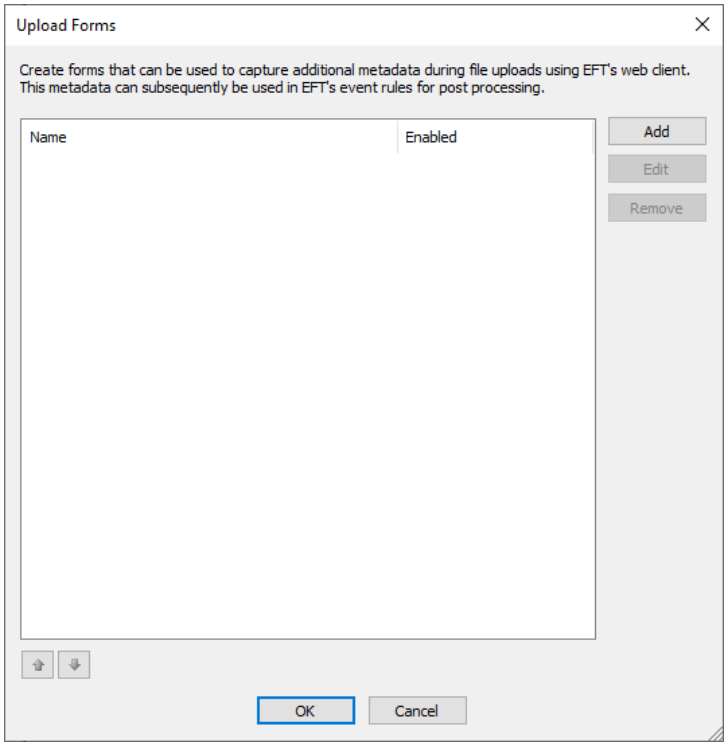
How do I create upload forms?

To create a form

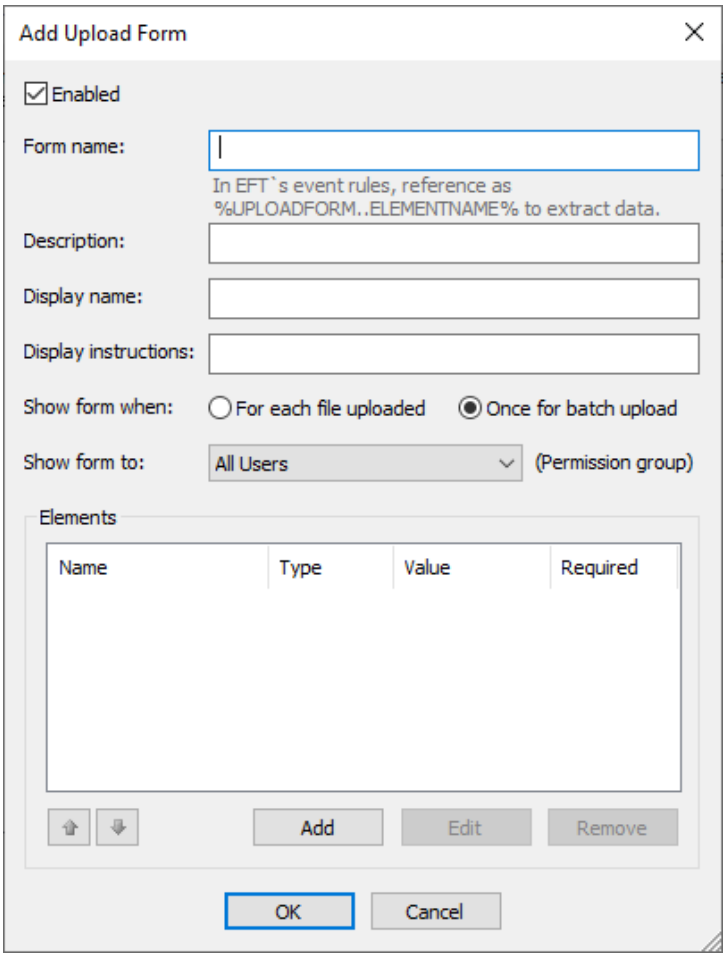
1. In the administration interface, connect to EFT and in the left pan, click the **Site**.
2. In the right pane, click the **Web** tab.



3. Next to Upload Forms, click **Configure**. The **Upload Forms** dialog box appears.



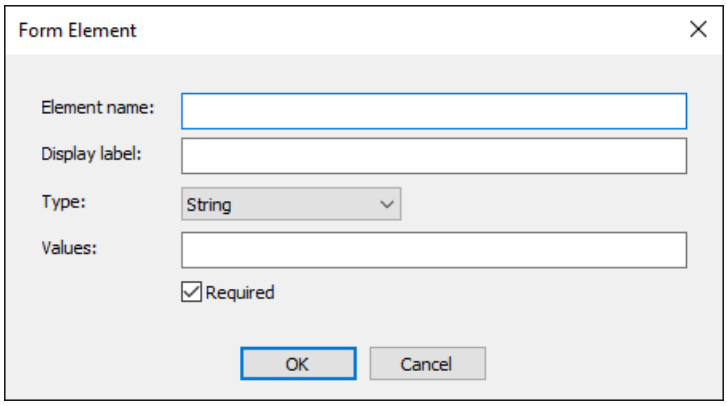
4. In the **Upload Forms**dialog box, you can **Add**, **Edit**, or **Remove**a form. You can also sort them using the arrow icons in the lower left.
5. To add a form, click **Add**. The **Add Upload Form** dialog box appears.



The **Enabled** check box is selected by default. If the check box is cleared, the form will not appear in the WTC.

6. In the **Form name**box, provide a unique name for the Upload Form.
7. (Optional) In the **Description**box, provide a description/purpose for this Upload Form.
8. In the **Display name**box, provide a name for the Upload Form that will appear in the WTC.
9. (Optional) In the **Display instructions** box, provide instructions for completing the form that will appear in the WTC.
10. Next to **Show form when**, specify whether to display the form **For each file uploaded**, or **Once for a batch upload**. The latter is useful if the metadata being provided will apply to all the files being uploaded as part of the batch.

11. Next to **Show form to,** specify the Permission Group that will see the form. If you need to show the form to a single user or small handful of users, you will need to create a Permission Group for those. If your Site is using Active Directory authentication (and authorization) then everyone will see the form, as currently there are no controls for only displaying the form to individual users.
12. The **Elements**section lists any added elements in the order they will be shown in the web form. You can change the order of the elements using the arrows, **Add** or **Remove**elements, or **Edit** existing elements. When editing or adding elements, the **Form Element** dialog box appears.



    a. In the **Element name** box, provide an element name (unique to this form) to be used as context variable name (defaults to field label). This value will be used by EFT's event rules as the "Element_Name" portion of the %UploadForm.Form_Name.Element_Name% variable.
    b. In the **Display label** box, provide a label associated with the element. This is displayed in the web form. (Form Elements must have labels to be in compliance with Section 508 standards for people with disabilities.)
    c. In the **Type**box, specify what type of value is used for the element: Drop-down list, Multistring, Radio buttons, String, or check box (Toggle).
    d. In the **Values**box, specify any values to appear for the drop-down list, radio buttons, or toggle names. Use commas to delimit multiple values.
    e. Select the **Required**check box, if this form is mandatory.
    f. Click **OK**to save the Element. If one or more mandatory fields is missing or invalid, a prompt appears: "One or more errors were encountered. Please enter all valid, required information and try again."
13. Create other Elements as needed.
14. Click **OK** to close the **Add New Form** dialog box.
15. Click **OK** to close the **Upload Forms** dialog box.
16. Click **Apply**to save the changes.

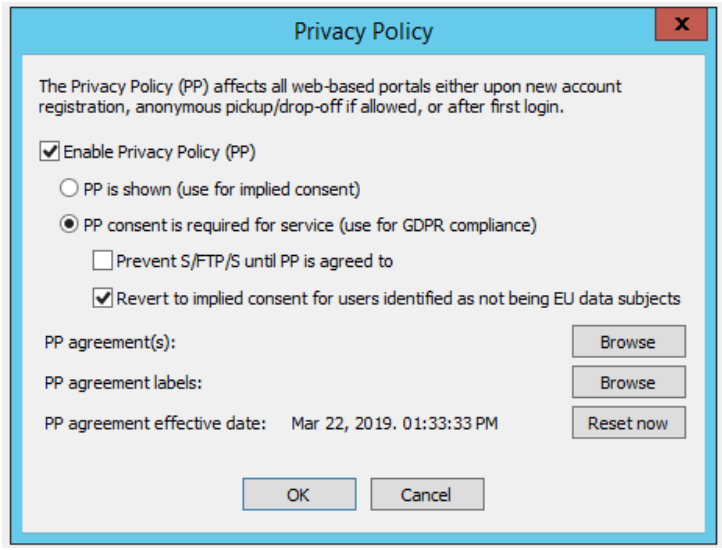
Privacy Policy

(Requires HTTP/S, Workspaces, RCM) You can create and display a Privacy Policy for all web-based access to EFT. The Privacy Policy affects all web-based portals upon new account registration, anonymous pickup or drop-off, and upon first login. For user-specific settings, refer to Specify Terms of Service and Privacy Policy Options.

- If accessing EFT for the first time via FTP, FTPS, or SFTP, and the Privacy Policy consent is required for use, the connection will fail. The user must first connect via the Web Transfer Client (HTTPS portal) to consent to the policy. The administrator can instead set the status for the Privacy Policy for a given user manually, on user account's **General**tab in the EFT administration interface. Additionally, you can change the EFT login banner to provide instructions to login via the Web Transfer Client before logging in via FTP, FTP, or SFTP.
- If the Privacy Policy is set to the default (enabled, but not mandatory) and the user implicitly agrees to the policy by continuing to use the service, then no record is audited to the EFT database.
- For anonymous users, accepting the Privacy Policy sets a cookie for 12 hours so that the user doesn't have to consent for each action within that 12 hours.
- For an example of a Privacy Policy, refer to https://policies.google.com/privacy.

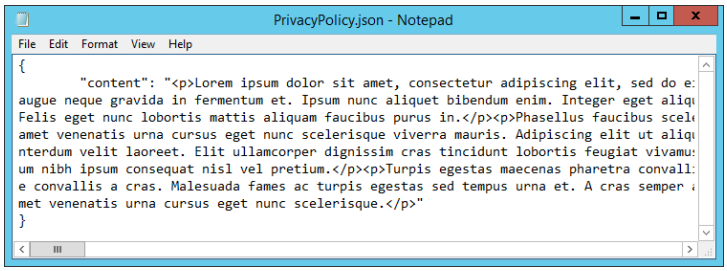
To enable the Privacy Policy agreement

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. On the **Web**tab, next to **Privacy Policy**, click **Configure**. The **Privacy Policy** dialog box appears.



4. Select the **Enable Privacy Policy** check box, then specify whether the agreement is **implied** or **required for service**. If the agreement is required, you can select the **Prevent** check box to prevent access over FTP, SFTP, or FTPS until the Privacy Policy agreement is accepted. The **Revert to implied consent for users identified as not being EU data subjects**is selected automatically.
5. To select or view the agreement(s) or the agreement labels, click **Browse**. Windows Explorer opens to the **\Web**folder.
6. The **\Templates**folder contains the **PrivacyPolicy.json**file. Replace the default text with your organization's Privacy Policy.

   The **PrivacyPolicy.json** file contains "dummy text" ("lorem ipsum dolor...") that you will replace with the text of your policy.



   You can use basic HTML formatting tags (<p>, <li>, etc.). The "content" label must be kept, as well as opening and closing curly brackets { } :

```
{
 "content": "<p>This is our Privacy Policy ... </p>"
}
```

7. Refer to **Edit the Privacy Policy and labels** for how to edit the Privacy Policy and agreement labels files.
8. To reset the agreement effective date, such as when publishing a new agreement, click **Reset now**.
9. Click **OK**, then click **Apply** on the **Web** tab. A Site restart is required.

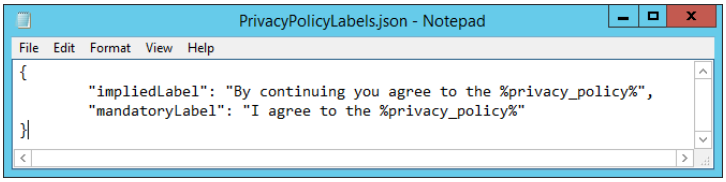
Edit the Privacy Policy and Labels

The **PrivacyPolicy** and **PrivacyPolicyLabels** files are JSON files (similar to XML) that must be edited for your organization's agreement. (The labels in the JSON file are case-sensitive.) The files are saved in:

C:\Program Files\Globalscape\EFT Server\Web\Templates

1. Open the **PrivacyPolicyLabels.json**file and the **PrivacyPolicy**.json file in a text editor, such as Notepad.
2. Save a copy of each before you edit the originals so you have a backup.

   The **PrivacyPolicyLabels** file is used to change the default text that appears when you have specified that the Privacy Policy is implied or when it's mandatory to continue. For example, the default text when the agreement to the policy is mandatory is, in English, "I agree to the Privacy Policy."



3. Change the value (By continuing...") to whatever your organization requires, or to another language. However, do not change any the label variables (impliedLabel, mandatoryLabel) or the text that is between the % signs. The opening and closing curly brackets { } are also required.

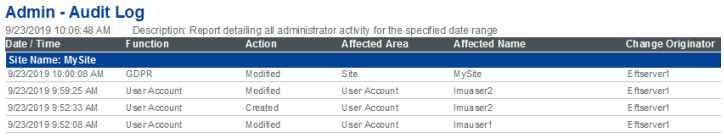
Related Topics

- Logging In (accepting Privacy Policy)
- Specify GDPR status, Terms of Service, and Privacy Policy Options
- GDPR Data Protection Officer
- GDPR Settings
- Terms of Service Agreement
- Specify Terms of Service and Privacy Policy Options

Privacy Reports

When changes are made to the GDPR settings, Privacy Policy, and Terms of Service, the changes are recorded in the database and can appear in reports.

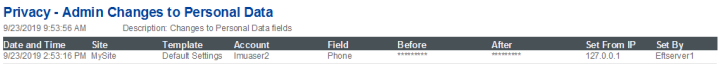
> **NOTE:** The Regulatory Compliance Module (RCM) is required for changes to GDPR, privacy, and terms of service data to appear in reports. The Auditing and Reporting Module (ARM), is required to run reports.



Admin - Audit Log

9/23/2019 10:06:48 AM Description: Report detailing all administrator activity for the specified date range

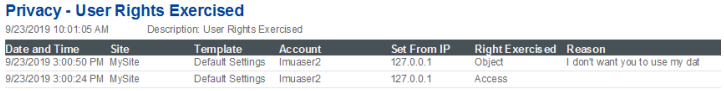
Date / Time	Function	Action	Affected Area	Affected Name	Change Originator
Site Name: MySite					
9/23/2019 10:00:08 AM	GDPR	Modified	Site	MySite	Eftserver1
9/23/2019 9:59:25 AM	User Account	Modified	User Account	Imuaser2	Eftserver1
9/23/2019 9:52:33 AM	User Account	Created	User Account	Imuaser2	Eftserver1
9/23/2019 9:52:08 AM	User Account	Modified	User Account	Imauser1	Eftserver1



Privacy - Admin Changes to Personal Data

9/23/2019 9:53:56 AM Description: Changes to Personal Data fields

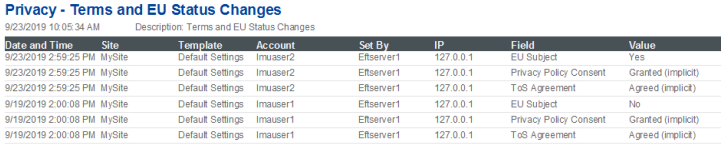
Date and Time	Site	Template	Account	Field	Before	After	Set From IP	Set By
9/23/2019 2:53:16 PM	MySite	Default Settings	Imuaser2	Phone	********	********	127.0.0.1	Eftserver1



Privacy - User Rights Exercised

9/23/2019 10:01:05 AM Description: User Rights Exercised

Date and Time	Site	Template	Account	Set From IP	Right Exercised	Reason
9/23/2019 3:00:50 PM	MySite	Default Settings	Imuaser2	127.0.0.1	Object	I don't want you to use my dat
9/23/2019 3:00:24 PM	MySite	Default Settings	Imuaser2	127.0.0.1	Access	



Privacy - Terms and EU Status Changes

9/23/2019 10:05:34 AM Description: Terms and EU Status Changes

Date and Time	Site	Template	Account	Set By	IP	Field	Value
9/23/2019 2:59:25 PM	MySite	Default Settings	Imuaser2	Eftserver1	127.0.0.1	EU Subject	Yes
9/23/2019 2:59:25 PM	MySite	Default Settings	Imuaser2	Eftserver1	127.0.0.1	Privacy Policy Consent	Granted (implicit)
9/23/2019 2:59:25 PM	MySite	Default Settings	Imuaser2	Eftserver1	127.0.0.1	ToS Agreement	Agreed (implicit)
9/19/2019 2:00:08 PM	MySite	Default Settings	Imauser1	Eftserver1	127.0.0.1	EU Subject	No
9/19/2019 2:00:08 PM	MySite	Default Settings	Imauser1	Eftserver1	127.0.0.1	Privacy Policy Consent	Granted (implicit)
9/19/2019 2:00:08 PM	MySite	Default Settings	Imauser1	Eftserver1	127.0.0.1	ToS Agreement	Agreed (implicit)

Display Full Name of User in the WTC

In the Web Transfer Client (WTC), you can display the full name of a user if the following settings are true:

- The Advanced Property"displayFullName" value must be set to "true" in administrator-configuration.json.
- GDPR Article 15: "Right of Access" must be set to "Exercised via EFT's Web Client"
- The user's full name must have a value in EFT (not an empty string)

If any of these settings are not true, the WTC will display the username on the account instead of the Full name.

C:\Program Files\Globalscape\EFT Server\Web\Shadowfax\portal\assets or

Changing the Language of the Client

EFT is used all over the world in a variety of languages. EFT has provided language files for some of the most-commonly requested languages. They are stored (by default) in **...\Program Files\Globalscape\EFT Server\Web\Shadowfax\wtc\assets\i18n** (The **\Web** directory is in the cluster share for HA installations.)

The international language (i18n) directory of the EFT installation folder includes the language files in JSON format.

- Instruct the user to specify their preferred language in the WTC in their user Profile.

This process for changing the language does not affect the EFT administration interface, just the Web Transfer Client after login. The initial login screen comes from EFT and is not localized.

Disable CRC

The Web Transfer Client (WTC) can validate the integrity of files transferred to and from EFT. Cyclical Redundancy Check (CRC32) is enabled on the WTC by default. The EFT administrator must have enabled CRC in its FTP configuration to take advantage of this feature.

With CRC enabled, when the WTC transfers a file to or from EFT, it automatically queries EFT for the CRC value of the file, then compares it to the CRC value for the local file. If they match, the transfer is reported as successful. If they do not match, the system reports a "CRC Failure." The user can then retry the transfer, if necessary. The client does not automatically retry the transfer if they do not match.

If upload verifications are not required, you can disable CRC in the WTC configuration file.

The HTML5 version of the Web Transfer Client does not support a CRC-check for downloaded files because of the limited access of html/js to the client file system. The process of initiating a download is human driven and can NOT be intercepted by a JavaScript API; it is wholly managed by the browser itself, for security reasons. Further, the browser cannot arbitrarily read files on the local file system (for obvious security reasons), so EFT cannot read contents of downloaded files to do CRC32, and thus cannot issue a follow-up HEAD request to verify the integrity of the download.

To disable CRC

1. Find the **admin-configuration.json**file.
    - In v8.0.5 and later: **\Web\Shadowfax\portal\assets**
    - In v8.1 and later: **\Web\Shadowfax\portal\assets**
    - The **\Web** directory is in the cluster share for HA installations.
2. Open the configuration file in a text editor, such as Notepad. (It may be necessary to change the extension from JS to TXT to view it properly.)
3. Find the following text:

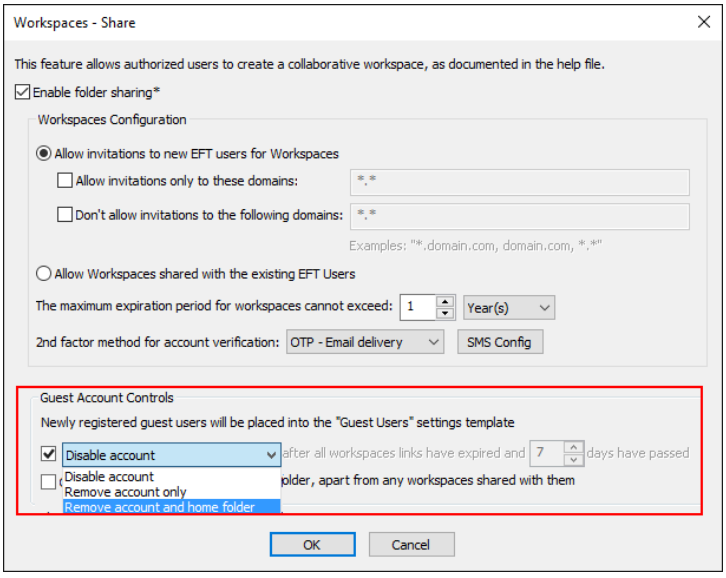
    ```
    "crcEnabled": true,
    ```
4. Change `true`to `false`, then save the file.
5. If you changed the name of the file to edit it, be sure to change it back.
6. Now transfers will be processed without CRC.

Guest Users

After a guest (non-EFT user) has been invited to join a Workspace, has created an account, and logged in, the guest account will appear (if so configured) in the **Guest Users** Settings template. The **Guest Users** Settings Template appears when Workspaces is enabled.

After the Workspace has expired, the guest account is either disabled or removed, depending on the settings on the **Site> Web > Folder sharing > Configure > Workspaces-Share**dialog box. If the guest account is disabled, the EFT administrator must remove it or enable it before they can receive any Workspaces invitations. Refer to "Guest Users" in Workspaces Invitations for details of re-enabling expired Guest accounts when new invitations are sent.

Guest users' permissions depend on what the EFT administrator configures in the Guest Users Settings Template. The default settings include **Download**, **Show this folder in parent list**, **Show files and folders in list**. Users with whom a Workspace is shared do NOT have permission to move files and folders out of the Workspace.



When password complexity is enabled and defined, a guest user's password might fail the complexity test and fail to create a user. In such cases, the user will receive an error message. The guest user should be instructed to create a password that meets complexity requirements defined by the EFT administrator.

Related Topics

- How Settings Templates Work
- Guest Users Settings Template

- Introduction to Permission Groups
- Sharing Folders (Creating a Workspace)
- Request Files
- Enable and Configure the Drop-Off Portal
- Edit-Remove Workspace Permission
- Transactional Workspaces

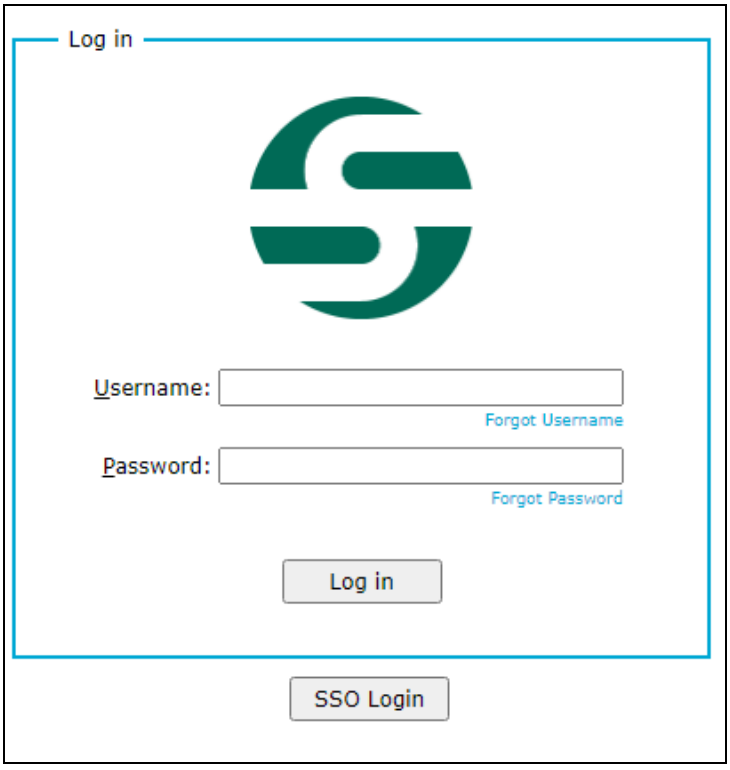
Logging In

You can log in to the WTC and Workspaces in any supported browser. The system administrator will provide you with the URL (web address) and your login information.

The EFT administrator should inform end users which IP address, port, username, and password should be used to log in to a Site. Because many users are unfamiliar with <IP address:Port> formatting, be sure to provide users with the exact URL that they should access to log in, whether they are accessing a Site from the Web Transfer Client, "plain-text" client, a command line, CuteFTP, or any other FTP client. For example, you could provide the link in an email.

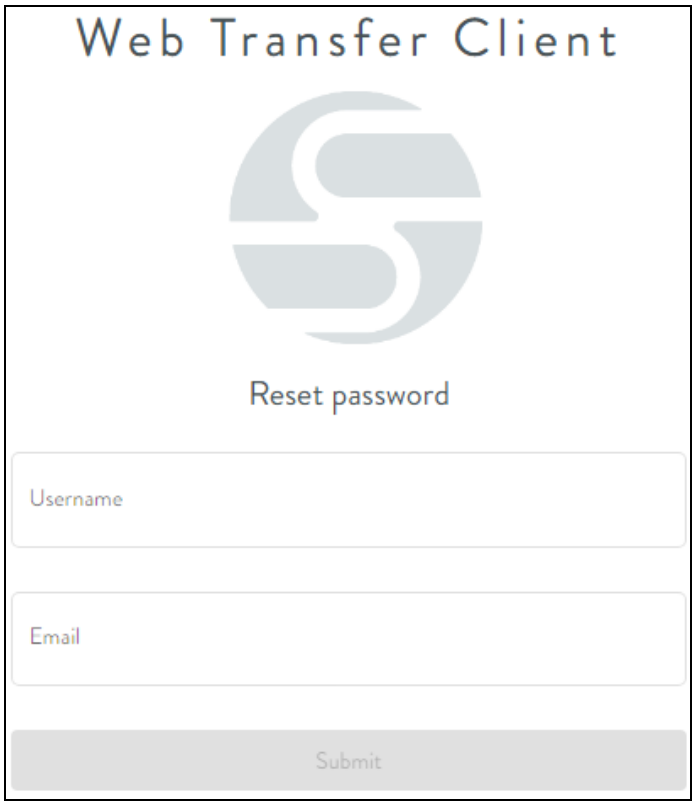
To log in

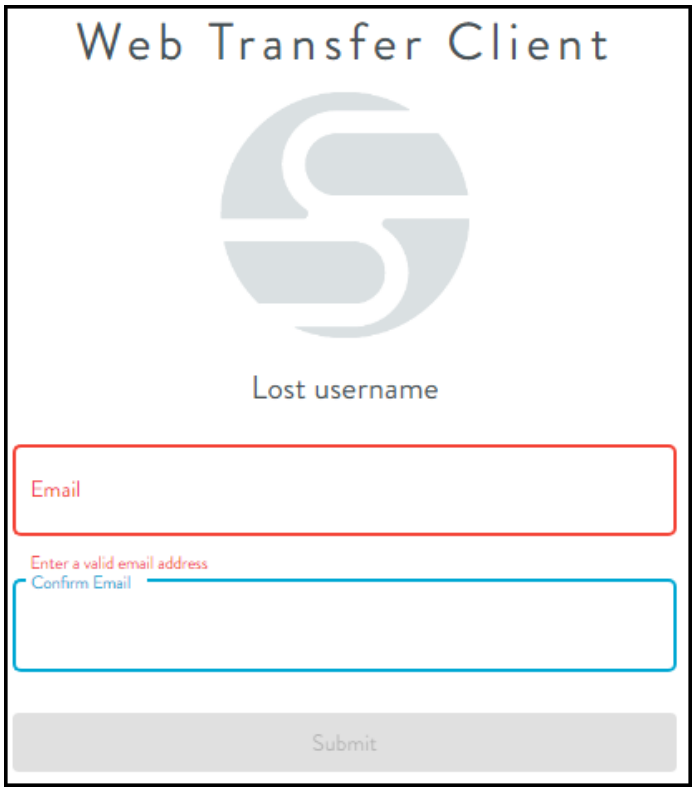
1. Open the web browser.
2. Type or click the web address provided to you by your system administrator. For example, type `https://www.ourfileserver.com`. The login page appears. (The **SSO Login** option appears if so configured.)



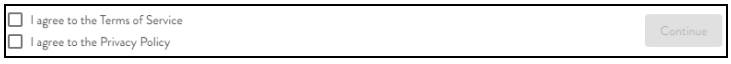
3. Provide your **Username**and **Password**, then click **Log In**. If you have been instructed to use secure sign-on, click **SSO Login**.

4. If you have been instructed to use two-factor authentication, you will be asked to provide a second response, such as a passcode. The EFT administrator can change the text that appears for the challenge. Refer to the article at https://kb.globalscape.com/KnowledgebaseArticle11267.aspxfor details.
5. If you don't know your username, click **Forgot Username** (if available). If you don't know your password, click **Forgot password**. In the dialog box that appears, provide your information and then click **Submit.**
    - If it is so configured in the EFT administration interface, users are prompted to change their password the first time they log in.
    - If a security prompt appears asking you to accept the website's certificate, select the **Always trust** check box, and then click **Yes**.
    - If a prompt appears to provide a passcode, use the method asked for in the prompt to retrieve your passcode (Email or SMS). In the dialog box that appears, provide your information and then click **Submit**. You will be asked for your email address to which the reset information will be sent. Your request is sent to the server and an automated response will email you your username.





- If you don't know your username, click **Forgot Username** (if available). Your request is sent to the server and an automated response will email you your username.
- If you don't know your password, click **Forgot password**.
- When the credentials are accepted by the server, the Web Transfer Client (WTC) appears.
- Depending on how the EFT administrator configured the WTC, you might see a box in which you can read and agree to the organization's Privacy Policy and Terms of Service.



- The administrator can configure EFT to require implicit or explicit agreement.
  - **Implicit** - Accept the agreement by using the WTC:
    - Click **Terms of Service** to read the agreement. Click anywhere outside of the agreement to close it.
    - Click **Privacy Policy** to read the policy. Click anywhere outside of the policy to close it.

    - Click the **X**to close the Terms of Service/ Privacy Policy box.
- **Explicit**- Select the **Agree**check boxes, and then click **Continue**.

Once you have accepted the agreement/ policy, your account information in EFT is updated to reflect your acceptance so that you don't have to accept the agreement/ policy every time you log in.

Related topic

- Logging Out
- Terms of Service Agreement
- Privacy Policy
- SAML (Web SSO) Authentication

Workspaces SSO Authentication

Workspaces can be configured to use SSO authentication (which can include JIT provisioning in the case of SAML SSO authenticated users) to be automatically directed to their Workspace or Pickup portal so that those users are not added as guest accounts.

Refer to SAML (Web SSO) Authentication more information about configuring SAML Web SSO authentication in EFT.

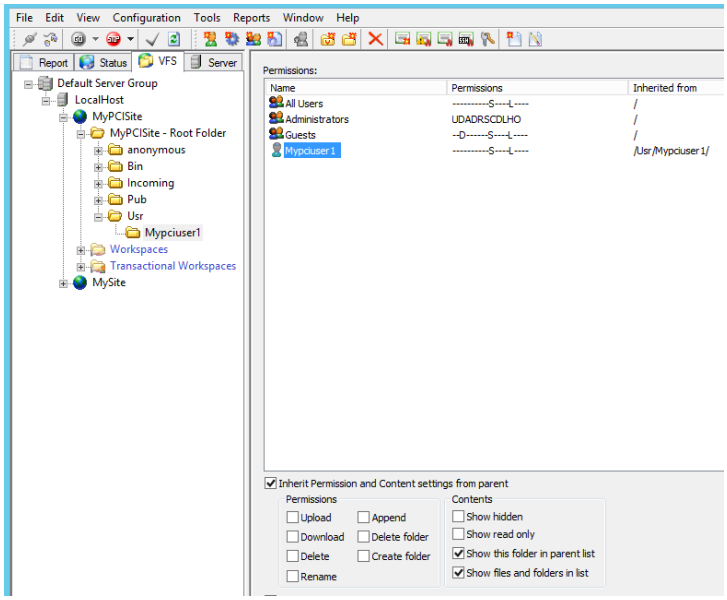
Managing Workspaces in the VFS

The **VFS** tab has a Workspaces view in which EFT Server- and Site-level administrators can:

- Delete shared Workspaces
- Add existing users to existing Workspaces
- Modify participant permissions of shared Workspaces
- When you send a file using the WTC, a "WorkspacesSendMessage" folder is created in the Virtual File System (VFS).
- The user account that is creating the Workspace must have the appropriate permissions on their home folder to create folders.
- You may have to refresh the administration interface to see any changes in the VFS tab (such as new Guest users and Workspaces added)

Sharing folders via the VFS tab

- Workspaces cannot be created via the **VFS**tab.
- External users cannot be invited via the **VFS**tab. External users can only be invited via the WTC.
- Users joined to Workspaces via the **VFS**tab, unlike users joined via WTC, are not sent invitation notification emails.
- Workspaces permissions may be granted via the **VFS** Workspaces view.



- The **VFS** tab will appear to permit all user permissions to be granted to a Workspaces participant. Suppose an EFT user creates a shared folder with only Upload permissions; an EFT administrator may invite participant1 to join the Workspaces folder, granting participant1 full administrative privileges to the folder. However, participant1 will receive an "access denied" response if they attempt to perform any actions within the folder other than upload, because the Workspaces folder respects the Workspaces owner's folder permissions.

Related Topics

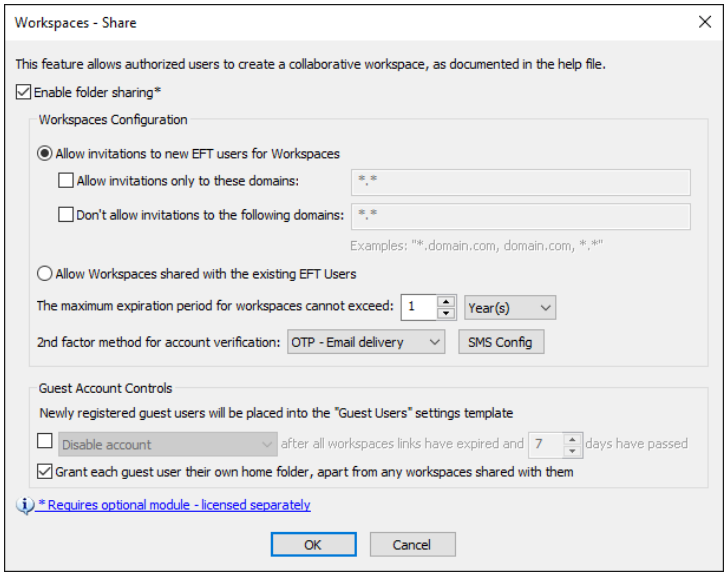
- Transactional Workspaces
- Workspaces Permissions

Restrict Workspaces Invitations to Specific Domains

(Requires HTTP/S, Workspaces) Administrators can configure Workspaces so that only specific domains can be invited to access a Workspace.

To restrict Workspaces invitations

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Web** tab.
4. Next to **Folder sharing**, click **Configure**. The **Workspaces - Share** dialog box appears.

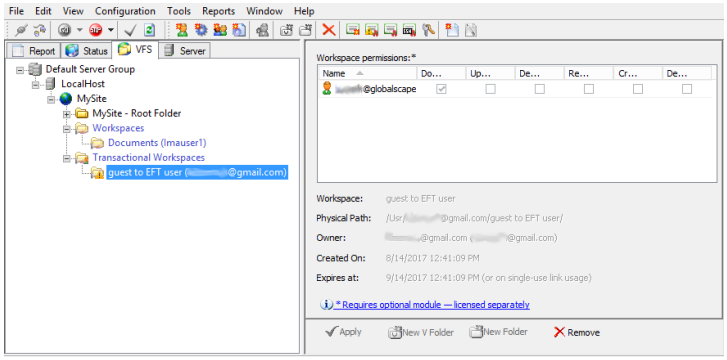


5. Select the **Enable folder sharing** check box and **Allow invitations to new EFT users for Workspaces** (if not already selected).

6. Select the **Allow invitations only to these domains** check box, then specify the domain(s) in the text box, comma/semicolon delimited. Wildcards are supported (for example, *.cisco.com or cisco.* or *.*). The setting is not selected by default.
7. Click **OK** to close the dialog box, then click **Apply**.

Transactional Workspaces

(Requires HTTP/S, Workspaces) A Transactional Workspaces is a special kind of Workspace that results from sending a file for pick up from the EFT Outlook Add-In or Drop-Off portal. The recipient only has download permission on the file(s) received. Transactional Workspace participants cannot see each other and cannot subscribe to notifications.



This Workspace is different from normal Workspaces in that a Transactional Workspace:

- Accepts anonymous access, if the administrator allows it and the owner/sender chooses
    - Contains folders in the VFS that have been shared via public links (unregistered users) and have an exclamation point on the anonymous-access folder
- Grants permission to download only
- Can't have participants added post creation
- Owner will have little power over it once created
- Is private access, in that participants can't see each other and can't subscribe to notifications (although owner/sender can)
- Is represented in the VFS tab using the Subject line and the sender's username
- Is represented differently in the WTC
- Content gets deleted when it expires
- Is more likely to have a shorter maximum expiration period than regular Workspaces
- Supports self-expiring, single-use file links, which are not supported in regular Workspaces

Related Topic

- Managing Workspaces in the VFS

Unicode File Transfers

EFT's support for UTF-8 encoded Unicode characters extends to:

Inbound protocols:

- HTTP/S
- SFTP

Event Rules:

- Copy/Move and Download action wizards (all protocols) when specifying "UTF-8" as the filename encoding, and when using wildcards for the source filename, e.g. (*.dat, or *.*)
- Advanced Workflow Engine when passed filename-related context variables (for example, %FS.PATH%, %FS.FILE_NAME%, etc.)

Auditing:

- EFT's summary Client Log (CL)
- EFT's extended client logs (e.g. LAN copy, FTP extended, and SFTP debug logs)
- EFT's debug log (Log4Cplus)

Exclusions*:

- FTP protocol (inbound)
- All Event Rule actions that process a filename related context variables (e.g. %FS.PATH%, %FS.FILE_NAME%, etc.); the only exception is Advanced Workflow module (AWM) actions
- Folder Monitor events. Windows will notify EFT when a Unicode file is dropped into a monitored folder, but EFT cannot (at present) pass the UTF-8 encoded filename context variable off to Event Rule actions for processing.

  The only exception being when the action is an AWM action, in which case UTF-8 encoding is preserved. Do not be tempted to use wildcards as the source filename for Folder Monitor rules (even if pollingonly is used), as this will lead to race conditions and other problems. Wildcards should only be used in rules that don't use filename context variables, such as Timer, user, or system related events.
- ARM database and all logs not explicitly mentioned above
- No User Interface (UI) components. This means you cannot specify Unicode characters in Event Rules or anywhere else in the administration interface
- No COM API support for Unicode
- EFT does not support UTF-8 filenames over AS2

*UTF-8 will be more comprehensive in a future version. Refer to Unicode Exceptions for more information.

Unicode FAQs

The FAQs below are provided to answer questions you may have regarding EFT's Unicode support.

Q. What is Unicode?

A. Unicode is a standard that provides a unique number for every character, regardless of platform, program, or language. Systems that don't support Unicode and without the proper ANSI code page will render characters such as 大きい魚 ???????. or .

Q. Does EFT support Unicode?

A. EFT partially supports Unicode and is moving towards full support.

Q. What about UTF-8?

A. UTF-8 is simply a popular mechanism for encoding Unicode characters using one or more bytes. Prior to supporting UTF-8, EFT used ANSI code pages to view filenames in the intended format (on the target system when browsing with the WTC or PTC).

Q. What other mechanisms for encoding Unicode characters does EFT support?

A. EFT uses full double byte UCS-2 encoding at the file system (I/O) level, UTF-8 encoding within EFT, and ASCII everywhere Unicode is not yet supported.

Q. Does EFT support UTF-8 for file transfers?

A. EFT preserves UTF-8 encoded filenames when transferring files over HTTP and SFTP when acting as a server, and over all supported protocols when acting as a client, when certain conditions are met (see next question).

Q. What about EFT's Event Rules?

A. EFT's Copy/Move and Download Action wizards (across all protocols) support Unicode when you specify "UTF-8" as the filename encoding method (radio button in the wizard), and when using wildcards for the source filename, e.g. (*.dat, or *.*). However, UTF-8 is not supported for these Actions if you use %FS.PATH% or any other variable for the source filename, which means the Folder Monitor Event cannot be used to offload files and conserve their Unicode format. In fact, the only Action that supports UTF-8-encoded filenames through context variables is an AWM workflow task.

Q. Which client applications can I use to see Unicode filenames when I transfer files to EFT?

A. EFT's Web Transfer Client (WTC) supports UTF-8. For file transfer applications that do NOT support UTF-8, Unicode filenames will appear as "???????.exe" when using them to transfer files to/from EFT. CuteFTP v9 supports UTF-8.

Q. Can EFT audit or log filenames or other data with Unicode characters?

A. EFT's summary Client Log (CL), extended client logs (LAN transfer logs, FTP logs, SFTP debug logs), and debug log (eft.log), and AWM logs all support Unicode characters. EFT's EX logs, cmd out logs, and ARM (both auditing and reporting) do NOT support Unicode characters.

Q. If this filename: 梅雨右折車線_XYZ.ISO is transferred to EFT, how will it appear on disk? In reports? In EFT's Event Rules?

A. EFT will store the file to disk and conserve the original Unicode filename. The filename will be audited properly to EFT's eft.log, but will be down converted to ASCII when audited to the EX log and to the ARM database, resulting in a filename that may look like this: ??????_XYZ.iso, which is also how it appears in EFT's reports. The reason the last three characters and file extension are conserved is that UTF-8 and ASCII characters are identical for English characters (A-Z). So there is no loss of meaning (fidelity) after performing a UTF-8-to-ASCII conversion. This same UTF-8-to-ASCII conversion applies when EFT hands off the filename to the Event Rule dispatcher, except where an AWM action exists, in which case the filename context variable will retain the original UTF-8 encoded filename. Thus if data integration of UTF-8 encoded filenames is needed, you should consider deploying AWM tasks alongside EFT's Event Rules.

Q How do Unicode filenames appear in EFT's administration interface?

A. EFT's administration interface (AI) does not support Unicode characters. UTF-8 is always down converted to ASCII in the AI. This means you can't specify a unique UTF-8 encoded filename in EFT's offload wizard, a UTF-8 encoded username, path, or anything else for that matter. The ONLY way to process Unicode filenames in the Copy/Move and Download Actions is to use wildcards (*.*, *.dat, etc.) as the source filename, instead of using a specific filename such as梅雨右折車線.ISO.

Q. Will Unicode encoded filenames be preserved in EFT Server's context variables, such as FS.FILENAME or FS.PATH?

A. Yes and no. For all Event Rule Events, Conditions, and Actions EFT will down convert the UTF-8 characters into ASCII. The only exception is when those variables are passed to AWM. In that case alone, EFT conserves the UTF-8 encoded filename, so that AWM can consume the original UTF-8 encoded filename, as AWM is fully UTF-8 compliant.

Q. Does EFT's internal handling of the file differ depending on whether the file was received in ASCII or Unicode?

A. In the guts of EFT it handles everything in Unicode. Conversion back to ASCII occurs only when working with a system or capability that doesn't support Unicode.

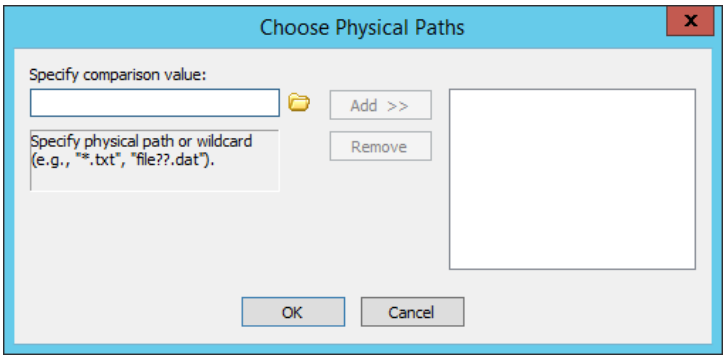
Related Topics

- IDN Support in EFT
- Unicode Exceptions

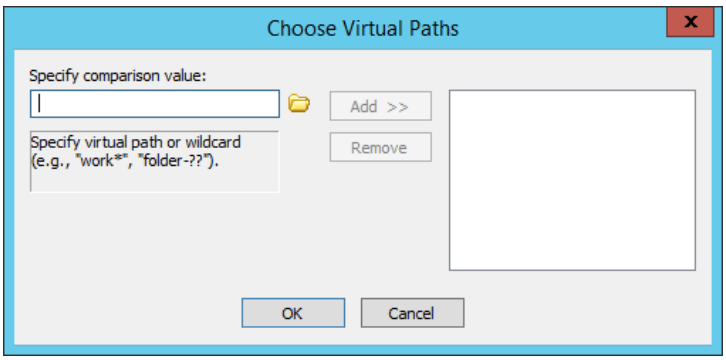
Workspaces Conditions

You can apply these Conditions to File Uploaded events.

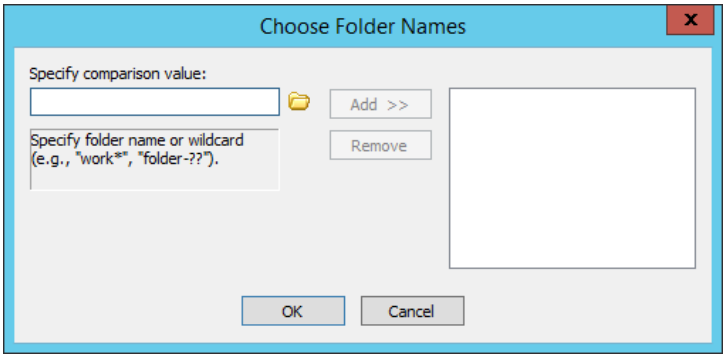
- **If Workspace Physical Path** - Tests whether the physical path does or does not match a path mask. Wildcards can be used.



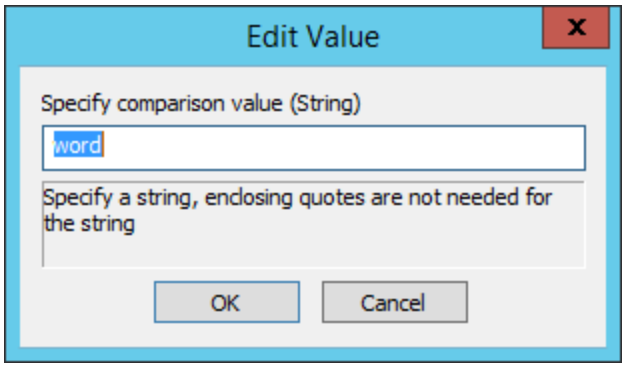
- **If Workspace Virtual Path** - Tests whether the virtual path does or does not match a path mask. Wildcards can be used.



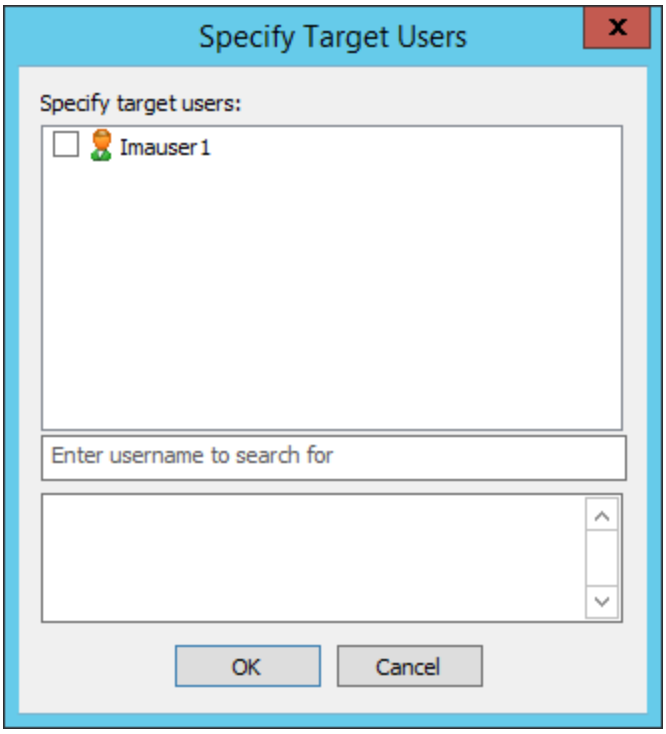
- **If Workspace Name** - Tests whether the folder name does or does not match a mask. Wildcards can be used.



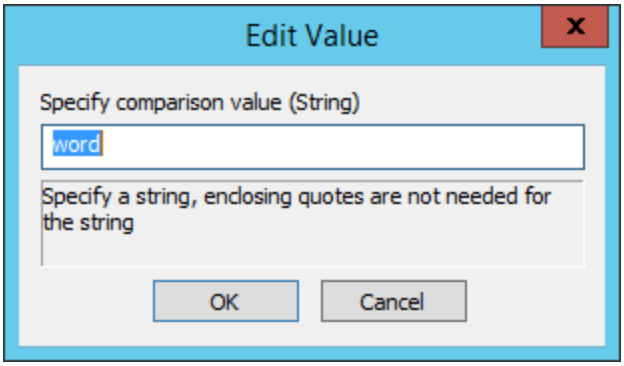
- **If Workspace Participants List** - Tests whether the participant list does or does not contain a string specified.



- **If Workspace Owner** - Tests whether the Workspace Owner is or is not one of a list of specified users.



- **If Workspace Owner Email Address** - Tests whether the Workspaces Owner email address does or does not contain or is equal to a specified string.



Workspaces Invitations

(Requires HTTP/S, Workspaces) An EFT administrator can invite internal users to join existing Workspaces in the **VFS** tab. External users cannot be invited via the **VFS**tab; they can only be invited by email address in the Web Transfer Client (WTC).

When a user is invited via the WTC, EFT follows the following logic flow:

1. EFT will first look for a matching email address in the existing Site user profiles and usernames. For example, let's say a Workspaces folder owner invites a user to share a folder with the email address test@gs.com. EFT will search for a user in the existing Site for either a username of "test@gs.com" or a username with an associated email of test@gs.com. If a match is found, then EFT sends an email to the invited user to let them know that they have been invited to share a Workspaces folder. Internal users are not invited, they are automatically joined.
2. If more than one internal user is associated with the invited email address, either by username or profile email address, EFT will decline to add the user.
3. If the email address is not associated with any internal username or email profile and the Site-level **Workspaces**tab has the **Allow invitation to new EFT users for Workspaces** option enabled, then EFT will add the user to the Workspaces folder as a "pending" user, and the user will be invited to create an EFT account to gain access to the shared folder. However, if the option is not enabled, then the invitation request will be denied.

Internal Users

When adding participants to Workspaces folders, the email address is the unique participant identifier. Existing users will be added to a Workspaces folder only if there is one and only one match for the email address being invited. Before completing an invitation, EFT will check both the username and email address fields for all users on the Site for matching addresses.

- **If two internal EFT users on the same Site have the same email address**, they cannot both be joined to the same Workspaces folder. For example, if user accounts test2 and test3 each have the email address user@gs.com, and the administrator attempts to add users test2 and test3 to a Workspaces folder, EFT will not permit test3 to join, and will state that it's due to duplicate users. In the WTC, the "Unspecified error has occurred" message will appear. If Workspaces trace level logging is enabled, then the log will report the offending email address.
- If one user's username is the same as another user account's email address and a Workspace owner attempts to invite that address, an error will occur and the user will not be invited.

Guest Users

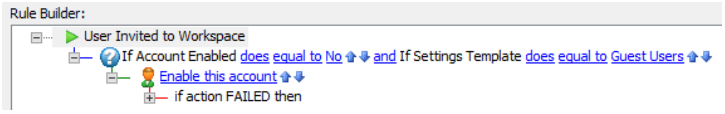
When guest users are invited to join a Workspaces folder, they must individually accept and activate each Workspaces invitation, then create an account to gain access to the Workspaces folder.

- When password complexity is enabled and defined, a guest user's password might fail the complexity test and fail to create a user. In such cases, the user will receive an error message. The guest user should be instructed to create a password that meets complexity requirements defined by the EFT administrator.
- When guest users join a Workspaces folder, their user accounts are created under EFT's Guest User Settings Template. Guest users are permitted to create Workspaces, but cannot invite new guest users to share the folder. Guest users can only invite users who already have an EFT account.
- The EFT **VFS** tab indicates which users are in the "pending" state, meaning they have not yet accepted their invitations. Once a user accepts an invitation, the "Pending" status is removed. Invited users have 5 days to accept and activate a pending invitation, after which the invitation will expire.
    - You can change the number of days with an Advanced Property named `WorkspaceInviteExpirationPeriodDays`. You can set it to any numerical value. If not set, the default is 5. If set to 0, the invite expiration

is the same as the Workspace link expiration.

If the Workspace invitation has expired before the invitee attempts to register, a prompt appears that says the invitation cannot be found.

- Workspace owners and EFT administrators are not notified when an user's invitation expires. When an invitation expires, the user is automatically removed from the Workspaces folder and no longer will appear as a pending user. To re-invite a user whose invitation has expired, the Workspaces owner, via the WTC, has to re-invite the user, at which point the invited user will go back into a pending status and will again have 5 days (by default; see Advanced Property above) to activate the account. Pending user status can only be viewed via the **VFS** Tab.
- A guest account that has been disabled (for example, due to the Workspace expiring) doesn't automatically get re-enabled if a new invitation is sent to them. If you send an invite to an account that was previously disabled by EFT due to expired links, EFT can re-enable the account via an Event Rule using the "User Invited to Workspace" event, the "If Account Enabled," "If Workspace User Account Exists," and "If Settings Template" is Guest Users Conditions, and the "User Account" action set to Enable this account:



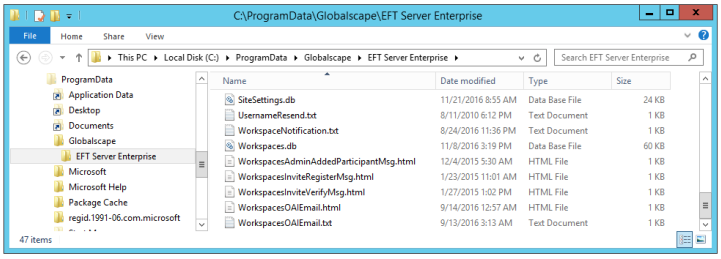
Workspaces Notifications

(Requires Workspaces module) When a Web Transfer Client user shares a folder, an invitation is sent to the user with whom the folder is shared. If the recipient does not have an account on EFT, the user can register the account. For invitations sent to non-EFT users, an email is sent to verify the account when the user registers the account.

The text for the invitation and verification emails is contained in an HTML file that can be customized for localization or to provide company-specific information.

Workspaces invitations expire after 5 days.

The templates are stored in **\ProgramData\Globalscape\EFT Server**or your cluster share under Templates, and apply to all Sites on the Server.



You can edit the files in any text editor. Note that the "WS" variables used in these notification templates are used only in these templates. They are not Event Rules variables. (Refer to Workspaces Events and Workspaces-Related Variables for additional means of notification.)

> **NOTE:** The Event Rules context variables are intended for use in the Event Rules subsystem. The Workspaces variables are not Event Rule variables and are outside of that subsystem. They are only used for Workspace notifications.

The files are named per their function:

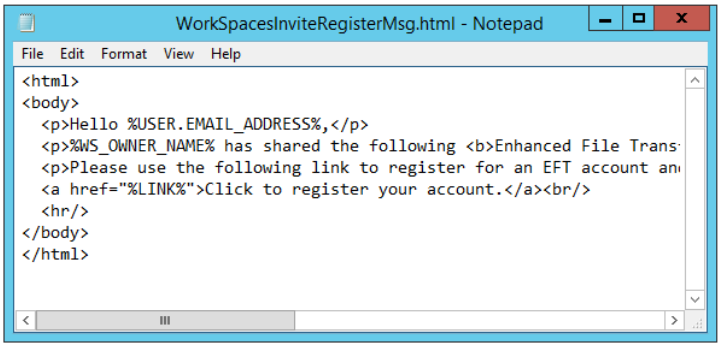
- WorkspaceNotification.txt - Used to notify the Workspace owner that a recipient took an action on a file.
- WorkspacesadministratorAddedParticipantMsg.html - Used to notify recipients that a Workspace was shared with them.
- WorkspacesInviteRegisterMsg.html - Used to notify recipients that a Workspace was shared with them and they are invited to register an account on EFT.
- WorkspacesInviteVerifyMsg.html - Sent after recipient has registered for an EFT account and needs to verify the account.
- WorkspacesOAIEmail.html - Notification to recipients that a file has been sent from Outlook.
    - WorkspacesOAIEmail.txt - Text version of the notification to recipients that a file has been sent from Outlook.
- WorkspacesOAIEmailWithSecureMB.html - Notification to recipients that a file has been sent from Outlook with secure message body.
    - WorkspacesOAIEmailWithSecureMB.txt - Text version of the notification to recipients that a file has been sent from Outlook with secure message body.
- WorkspacesRequestFileEmail.html - Notification to sender that a file has been requested.
    - WorkspacesRequestFileEmail.txt - Text version of the notification to sender that a file has been requested.

The following variables can be used in Workspaces notification templates:

Variable	WorkspaceNotification.txt	WorkspacesAdminAddedParticipantMsg	WorkSpacesInviteRegisterMsg	WorkSpacesInviteVerifyMsg	WorkSpacesInviteVerifyMsg2	WorkspacesOAIEmailWithSecureMB	WorkspacesRequestFileEmail
%WS_OWNER_NAME%		✓	✓				
%FOLDER_NAME%		✓					
%WS_FOLDER_NAME%	✓		✓				
%FILE_ACTION%	✓						
%RECIPIENT%	✓						
%RECIPIENTS%					✓	✓	
%RECIPIENT_IP%	✓						
%CC_RECIPIENTS%					✓	✓	
%ACTION_DATE%	✓						
%ACTION_TIME%	✓						
%USER.LOGIN%		✓	✓				
%USER.FULL_NAME%							
%USER.EMAIL_ADDRESS%			✓	✓			
%LINK%		✓	✓	✓			
%LINK_DOMAIN%			✓	✓			
%LINK_PATH%			✓	✓			
%WS_MESSAGE%		✓	✓				
%VERIFICATION_LINK%				✓			
%PASSCODE%				✓			
%WORKSPACE_LINK%					✓		
%DATE_EXPIRE%					✓	✓	
{{SENDER}}							✓
{{REPLY_URL}}							✓
{{EXPIRE_TIME}}							✓
{{SENDER_MESSAGE}}							✓

To edit the Workspaces invite and verify messages

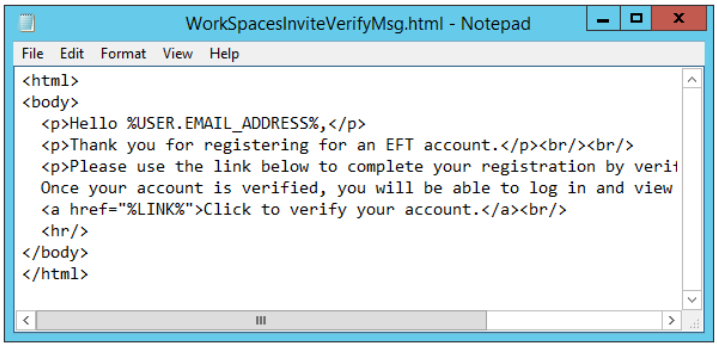
1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the **Server** node.
3. In the right pane, click the **General**tab.
4. In the **General Settings**area, next to **Workspaces invite message**, click the browse icon. Your default text editor (for example, Notepad) opens with the invitation text in HTML.



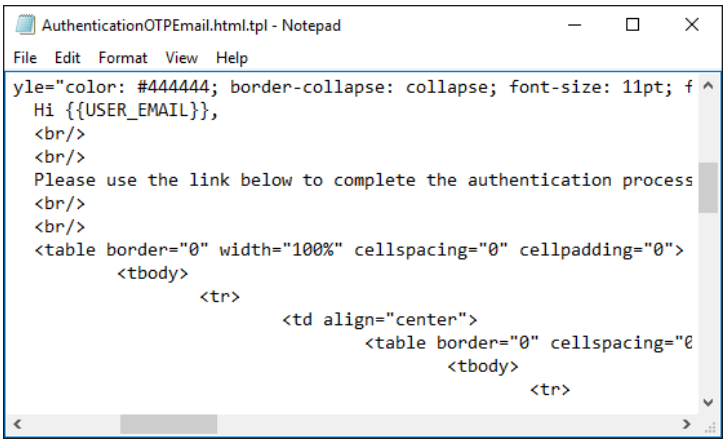
Edit the text as needed, being careful not to delete the variables (%USER.EMAIL_ADDRESS%, %WS_OWNER_NAME%, %FOLDER_NAME%, %LINK%), then save the file and close the text editor.

The WS_ variables are not Event Rule variables. To use Workspaces variables in Event Rules, refer to the Variableslist.

5. Next to **Workspaces verify message**, click the browse icon. Your default text editor (for example, Notepad) opens with the verify text in HTML.



6. Edit the text as needed, being careful not to delete the variables (%USER.EMAIL_ADDRESS%, %LINK%).
7. In the **General Settings**area, next to **Authentication OTP message**, click the browse icon. Your default text editor (for example, Notepad) opens with the message text in HTML.



8. Edit the text as needed, being careful not to delete the variables, such as {{USER.EMAIL}}, then save the file and close the text editor.
9. Save the file and close the text editor.

To create Site-specific versions

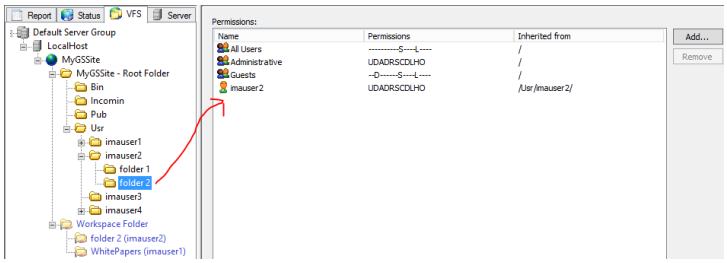
(See also Specifying External and Internal Domains)

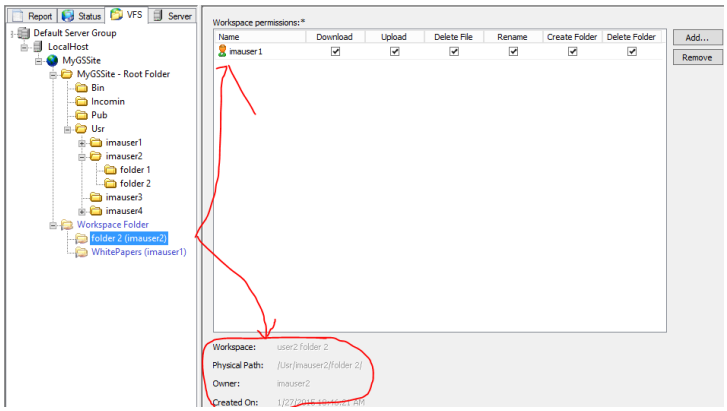
1. Make a copy of the existing template.
2. Make your edits (using a text editor, such as Notepad), being careful not edit any of the variables or necessary code.
3. Save the edited version with the Site name and an underscore prepended to the front if the filename. For example, name it `MyFrenchSite_PasswordResetMsg.html`

Workspaces Permissions

Workspaces permissions are separate from the VFS permissions, such as those permissions for the **Usr**folders. Users who have Workspaces permissions on a folder will not appear in the VFS permissions for that folder. For example (as shown below):

1. "imauser2" has full permissions on the \Usr\imauser2\ folder in VFS.
2. In Workspaces, "imauser2" has shared a folder called "folder 2" with "imauser1."
3. When the administrator clicks "folder 2" in the Workspace Folder tree, you can see that "imauser1" has Workspaces permissions on that folder.
4. However, only "imauser2" has VFS permissions on that folder.





Workspaces Permissions on an Active Directory Site

Workspaces has the ability to invite external users on an Active Directory Site. Described below is what occurs when a non-AD account has been invited to a Workspace, what permissions the EFT Server enforces for file activity, and how that applies to the "Comments" feature of Workspaces. This is important because the basic behavior of an AD Site, independent of Workspaces, is that any client that logs in as an AD account will subsequently access all files exposed by EFT's protocol engines using that very same AD account used to log in (known as "impersonation"). Thus, it is

not EFT that enforces file system permissions to local and UNC paths; it is the Windows operating system.

When EFT allows non-AD users to gain access to this Site (when we allow invitations to external parties) then we no longer impersonate an AD user and, therefore, our EFT application is limited in access by the service account under which it runs; ***however,*** this might be more permissive than the permissions for any individual user in the AD server.

For example, suppose your organization's AD users have READ/WRITE access to everything on a shared drive, and have explicit DELETE permission to our own folder but no one else's folder. Suppose the IT administrator set up a Folder Monitor rule against the shared drive. The IT administrator would have to run the EFT service as an AD account that had READ/WRITE/DELETE permissions across the whole shared drive so that the Folder Monitor workflows can move or delete files, or so that the EFTArchive operation worked, and so on.

Suddenly, there is a security concern: Any externally invited Workspace user will act against the shared drive the same as the EFT service account, not an individual AD account.

Therefore, our application itself must impose permissions checks on all file access for such accounts (which, by the way, is exactly how LDAP, Local, and ODBC authentication work).

EFT server will perform a permissions check on any assignment of Workspaces permissions to a participant (creation or modification time). EFT compares the OWNER permissions to the requested Workspaces permissions for a participant, and ensures at that moment that the OWNER does not grant MORE permission to a given folder than that which the owner of the folder holds.

All file activity within a Workspace is managed by EFT to conform to ONLY those permissions allowed by the Workspace configuration. Therefore, EFT enforces that Workspace permissions are equal to or less privileged than the owner's permissions, regardless of the service account under which EFT operates.

Below is a summary table that describes the permissions checks EFT applies to Workspace file and Comments activity for both **OWNERS** and for **PARTICIPANTS** upon adding or modifying participants in a Workspace:

Operation on file or comments	Required Owner EFT VFS permissions	Required Participant Workspace permissions
ADD	PERMISSION_FILE_APPEND or PERMISSION_FILE_UPLOAD	canUploadFile

Operation on file or comments	Required Owner EFT VFS permissions	Required Participant Workspace permissions
UPDATE	PERMISSION_FILE_APPEND or PERMISSION_FILE_UPLOAD	canUploadFile
DELETE	PERMISSION_FILE_APPEND or PERMISSION_FILE_UPLOAD	canUploadFile
GET	PERMISSION_DIR_LIST	N/A – Means that Participant can read comment because Owner invited them to Workspace.

For example, for the invited user to be able to comments to files, ***both*** of the following conditions must be met:

- Owner must have **Append**or **Upload** EFT VFS permission for that file.
- Participant (invitee) must be granted the **Upload**Workspace permission by the inviter.

Workspaces-Related Variables

The variables below are for use in Event Rules for virtual/physical path, owner, and so on. The Workspaces notifications use different variables than these, as shown below.

Text Displayed	Variable	Value Contained in Variable
Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%	Virtual path of the Workspace
Workspace Physical Path	%WORKSPACE.PATH%	Physical path of the Workspace
Workspace Name	%WORKSPACE.NAME%	Name of the Workspace Folder
Workspace Participants List	%WORKSPACE.PARTICIPANTS%	Participants sharing the Workspace
Workspace Subject	%WORKSPACE.SUBJECT%	Subject line of the email sent via Workspaces
Workspace Message	%WORKSPACE.MESSAGE%	Message sent via Workspaces
Workspace Owner	%WORKSPACE.OWNER%	Owner of the Workspace
Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%	Email address of the owner of the Workspace; the variable is case sensitive when used in the To, Cc, or Bcc fields of email notifications.
Workspace User	%WORKSPACE.USER_NAME%	Username of the Workspace participant
Workspace User Permissions	%WORKSPACE.USER_ PERMISSIONS%	User permissions of the Workspace
Workspace User Email Address	%WORKSPACE.USER_EMAIL%	User email of the participant
Workspace User Account Exists	%WORKSPACE.USER_ACCOUNT_ EXISTS%	Identifies whether the user account exists (or needs to be created)

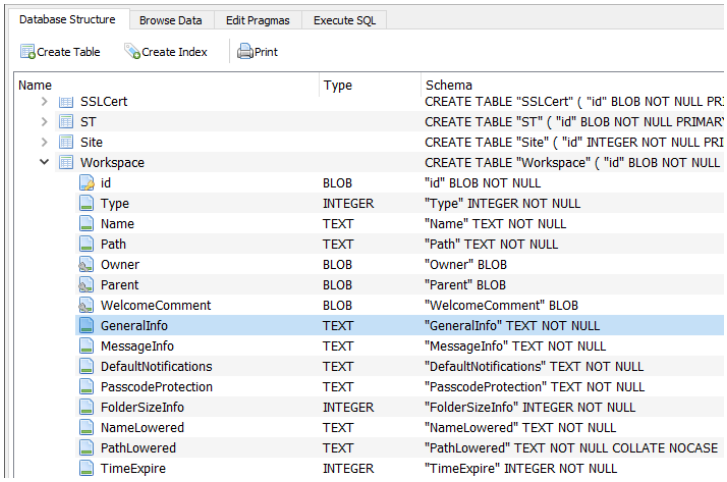
Viewing Data in DB Browser

All EFT data is stored in SQLite database files. You can view this data in a utility called DB Browser. The .DB files contain statistics and configuration data about the server and the site(s).

- **ServerStats.db** and **SiteStats.db** contain statistics about the Server and Site from which you can generate data to provide to Globalscape Support.
- **ServerConfig.db** contains configuration information found on the **Server**tabs, such as server status, listening IP, administrator access and permissions, SSL, FIPS, logs, database settings, SMTP settings, and HA information.
- **SiteConfig<GUID>.db**contains configuration information found on the **Site**tabs, such as Site connection information, security settings, web portals configuration, and Workspaces configuration.

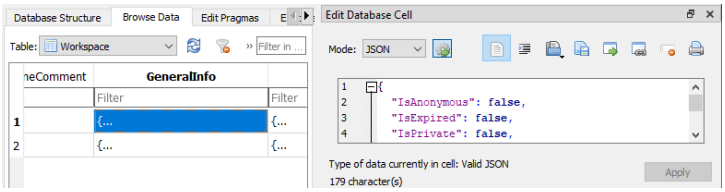
To view Workspaces data in DB Browser

1. Open the **SiteConfigDB** file (such as SiteConfig.e1b88396-e1e0-4e5d-b7ce-f43ab008f0b5.db) in DB Browser.
2. There are several columns in the tables. For example, in Workspaces, the columns are **id**, **Type**, **Name**, **Path**, **Owner**, **Parent**, **Welcome Comment**, **General Info**, **MessageInfo**, and others. Most are self-explanatory, such **Owner** is the Workspace Owner, **Name** is the name of the shared folder. **Path** is the location of the shared folder, and so on.
    - You can also see these columns in the **Data Structure** tab:



3. In DB Browser, select the **Table** drop-down list, then click **Workspace**.

4. To view the data in cells that have a curly brace and an ellipsis **{...** , double-click the cell. The data appears in the **Edit Database Cell** pane on the right side of the interface.



For example, in the **GeneralInfo** column, the cell might contain the following information:

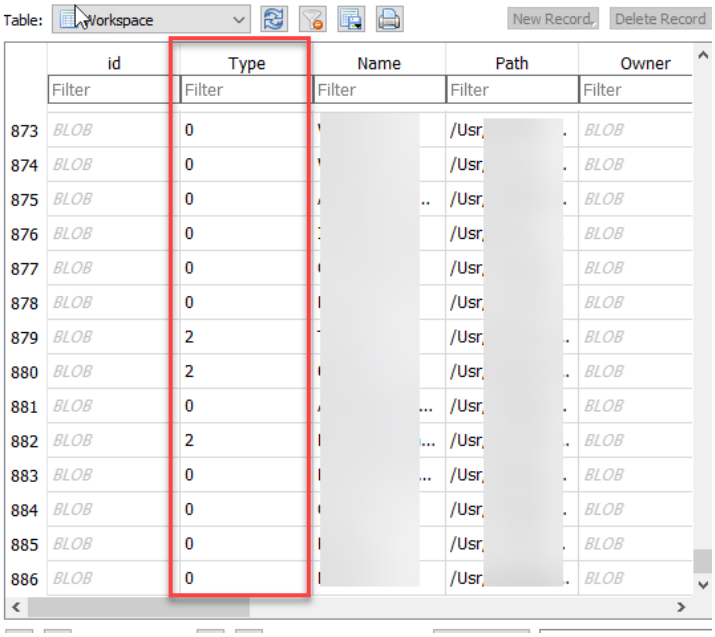
```
{
  "IsAnonymous": false,
  "IsExpired": false,
  "IsPrivate": false,
  "IsSingleUse": false,
  "State": "Complete",
  "TimeCreation": 1715288342,
  "TimeExpiration": 1746824342
}
```

The **MessageInfo** column might contain data such as:

```
{
  "Attachments": [],
  "BaseReplyDuration": {
    "Units": "Hour",
    "Value": 0
  },
  "BccRecipients": [],
  "CcRecipients": [],
  "EmailFrom": {
    "EmailAddress": "",
    "Name": ""
  },
  "IsAnonymousReplyAllowed": false,
  "Message": "",
  "SecureMessageBody": false,
```

```
  "Subject": "",
  "ToRecipients": []
}
```

Some columns, such as the **Type** column, contain numbers, such as:



The **Type** column displays numbers called *enums* which indicate that the row represents one of the following:

- 0 = Folder Share
- 1 = Workspace Outlook workspace
- 2 = Transactional Workspace (send)
- 3 = Workspace Reply
- 4 = Workspace Drop Off
- 5 = Workspace Request

Related topic

- EFT DB Files

Using the EFT Outlook Add-In

This section provides information about using the EFT Outlook Add-In.

- Introduction to the EFT Outlook Add-In
- Installing the EFT Outlook Add-In
- EFT Outlook Add-In Interface
- Changing the Message Format in Outlook
- Connecting to EFT from Outlook
- Configuring Message Options in Outlook
- Enabling or Disabling the Outlook Add-In in Outlook
- Enabling Outlook's Language Detection
- Mail Profiles with Multiple Accounts
- Recovering an Email from "Unrecoverable Error"
- Sending Files with the Outlook Add-In
- Viewing Add-In Status

Introduction to the EFT Outlook Add-In

EFT Workspaces includes an Outlook Add-In that allows you to send files in Outlook using Workspaces. If you have ever sent an email with attachments, you already know how to use the Outlook Add-in. Create the email, attach one or more files to the email, then click **Send**. You will continue to send and receive emails as always; the only difference is that the Outlook Add-in works transparently in the background to transfer the emails that have attachments.

Related Topics

- Installing the EFT Outlook Add-In
- EFT Outlook Add-In Interface
- Changing the Message Format in Outlook
- Connecting to EFT from Outlook
- Configuring Message Options in Outlook
- Enabling or Disabling the Outlook Add-In in Outlook
- Enabling Outlook's Language Detection
- Mail Profiles with Multiple Accounts
- Recovering an Email from "Unrecoverable Error"
- Sending Files with the Outlook Add-In
- Viewing Add-In Status

Installing the EFT Outlook Add-In

To use the Workspaces with Outlook, you must first install the EFT Outlook Add-In. You can use the deployment script available on the **Workspaces File Send** tab of the Site to deploy it to multiple computers at once in any deployment tool that you normally use, or you can install it with the EFT Outlook Add-In installer as described below.

> **NOTE:** If a "Publisher cannot be verified" prompt appears during the installation of the EFT Outlook Add-In, ensure that you are using the latest version of Microsoft Office 2019.

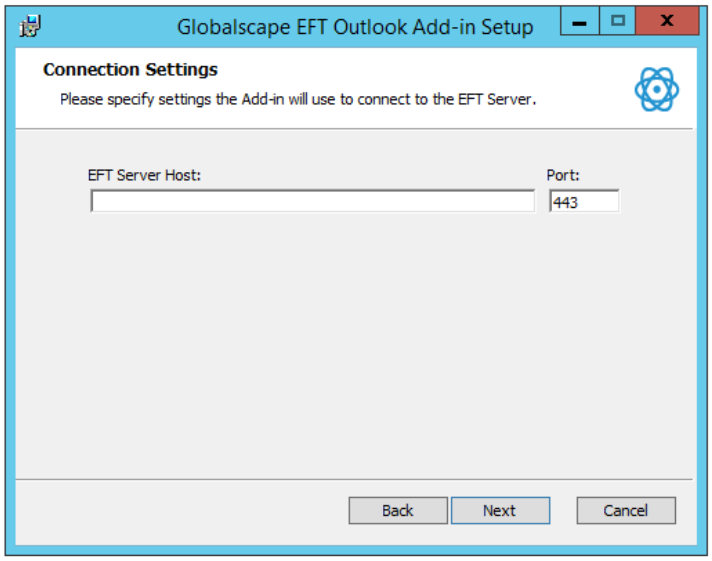
Before installing, refer to the system requirements.

When configuring Outlook to send files with Workspaces, ensure the following configuration is set:

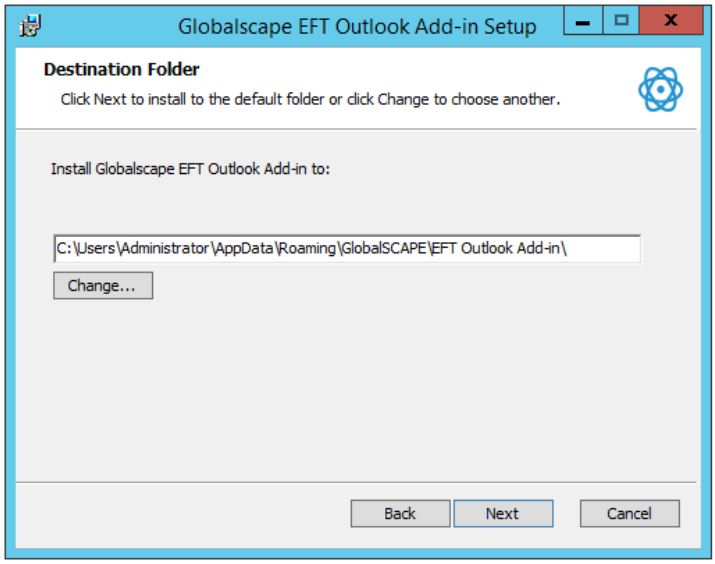
- The user account must have **Allow Secure File Sending** enabled on the user account's **Connections** tab.
- Kerberos requires the administrator to set the SPN for the account EFT is using.
- All user accounts need folder creation at their root folder enabled.

To install the EFT Outlook Add-In

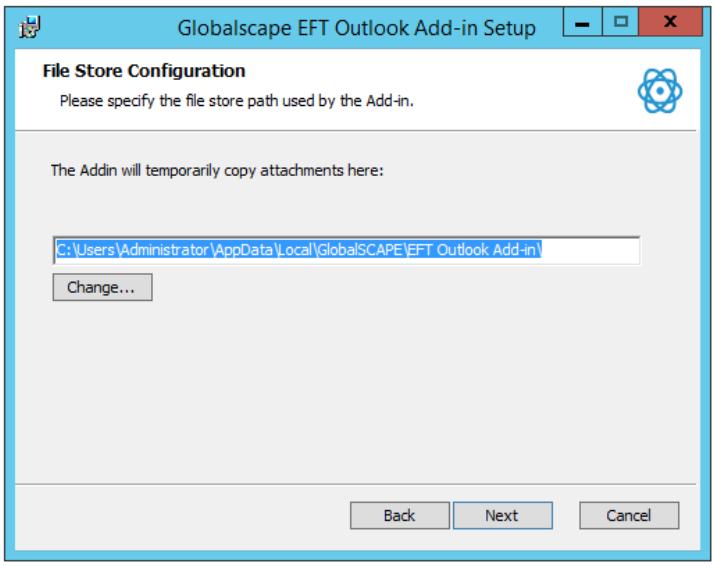
1. Get the installers from the installation folder (for example, C:\Program Files\Globalscape\EFT Server\OAI).
    - **EFTOutlookAddinInstaller.msi**- This is the main installer.
    - **EFTOutlookAddinSetup.exe**- This executable contains files that are needed by the main installer.
2. Start the **EFTOutlookAddinInstaller.msi**installer and click **Next** on the Welcome page.
3. Click **Next**.



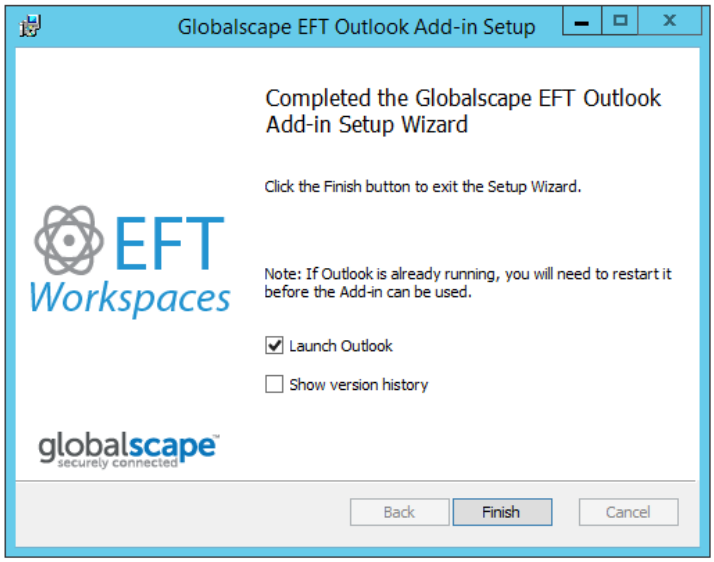
4. Specify the **EFT Server Host**(URL) and **Port**, then click **Next**.



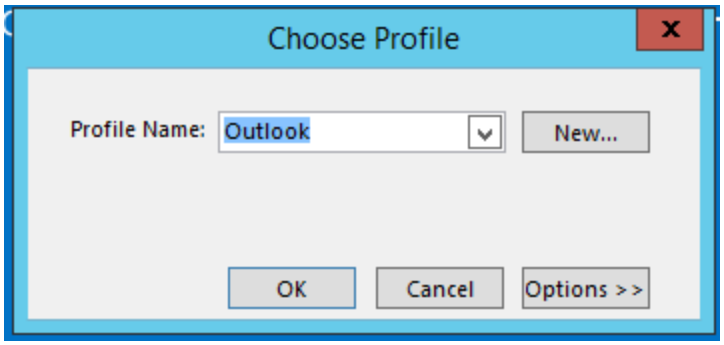
5. Specify the location in which to install the Add-In, then click **Next**.



6. Specify the location to store temporary copies of attachments while they are processed, then click **Next**.
7. Click **Install**.



8. When installation is complete, click **Finish**. Outlook is launched.
9. In Outlook 2013 and 2016, the **Choose Profile** dialog box appears.

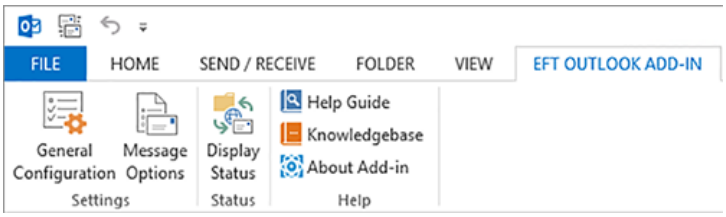


10. Specify which profile you want to configure for use with the EFT Outlook Add-In, then click **OK**.
11. When Outlook opens, it will ask if you want to install the Add-In. Click **Yes**.
12. If there are issues with the EFT SSL certificate, you will be ask if you want to accept it. Click **Yes**. (Clicking **No** will disable the Add-In.)

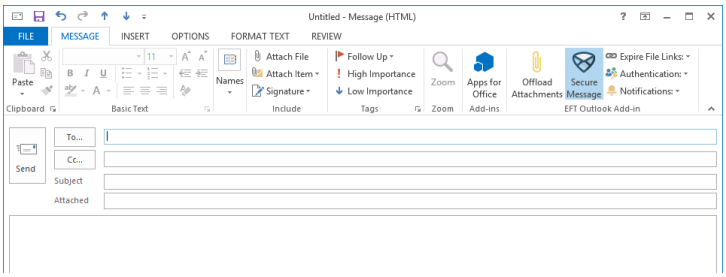
    The EFT Outlook Add-In options appear on the menu and in new emails.

EFT Outlook Add-In Interface

The EFT Outlook Add-In allows you to send files from Outlook for pickup via a secure link. When the user interface is enabled, the EFT Outlook Add-in options are available in Outlook:



When you create a new email, the EFT Outlook Add-In options appear:



- If the EFT Outlook Add-in does not appear in Outlook, refer to Enabling or Disabling the Outlook Add-In.
- If the EFT Outlook Add-in options are unavailable, check the following settings:
  - The account used to connect to EFT is not valid. Be sure that an EFT user account is used to connect to EFT.
  - The Add-in is unable to communicate with the EFT server. This could be caused by a number of issues, including incorrect connection information, invalid or blocked user account, or blocked IP address from multiple invalid connections.
  - Outlook Add-in is disabled in Outlookor in EFT.

Related Topics

- Installing the EFT Outlook Add-In
- Workspaces for Outlook

Changing the Message Format in Outlook

The procedures below describe how to change the message format, depending on your version of Outlook.

To change the message format for all messages

1. Click the **File** tab.
2. Click **Options**.
3. Click **Mail**.
4. Under **Compose messages**, in the **Compose messages in this format**list, click **HTML** or **Plain Text**.

To change the format of an individual outgoing message

1. With the message open, on the main menu, click **Format Text**.
2. On the **Format** tab, click the format you want to use (**Plain Text** or **HTML**).

> **NOTE:** Rich Text-formatted (RTF) messages are not supported.

Connecting to EFT from Outlook

Typically, the EFT Outlook Add-In server connection information is configured by the administrator. You should not edit these settings unless directed to do so by your administrator. EFT administrators should also refer to Configure a Service Principal Name SPN for Windows Authentication, below, to configure Integrated Windows Authentication (Kerberos).

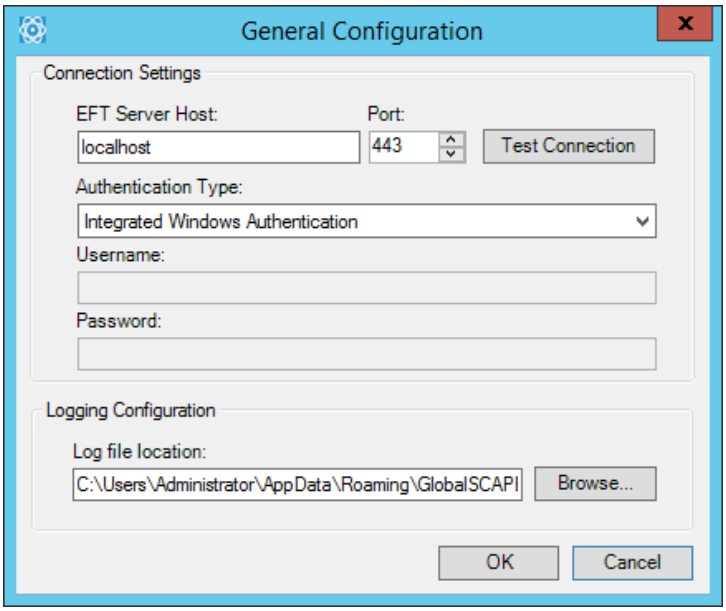
You might want to edit these settings are if your username/password has changed, if the server is moved to another host, if your login type was changed, or if you need to change the log file location.

If the EFT Outlook Add-In is not connected to the server, it will not try to upload packages.

In the **General Configuration**dialog box, accessed from the EFT Outlook Add-In toolbar/ribbon, you can specify to which server you want to connect, how to authenticate your connection, and where to save log files. In most cases, your administrator will configure this for you during setup.

To configure the EFT Outlook Add-In

1. On the **EFT Outlook Add-In** toolbar/ribbon, click **General Configuration**. The **General Configuration** dialog box appears.



2. In the **EFT Server Host** box, provide the host name of EFT.
3. In the **Port**box, provide the port used by EFT for HTTPS connections.

In the **Authentication type** box, specify either manual or Windows authentication:

4.

- **Manual**—You must provide the username and password that you use to connect to EFT or your AD credentials.
  a. In the **Username**box, provide the *username that you use to connect to EFT* or your AD username.

     In the **Password**box, provide the *password that you use to connect to EFT* or your AD password.
  b.

     Use the EFT login credentials for the EFT user account, not the administrator.

- **Integrated Windows Authentication**—Used this login type if you connect to EFT via Single Sign On (Kerberos). In this case, you do not need to provide a username and password. Your Windows credentials are used to connect.

5. If you want to test your connection, click **Test Connection**.
6. (Optional) In the **Log file location** box, specify the path at which the log file is saved.
7. Click **OK** to save your changes, or click **Cancel**if you do not want to save your changes.

Configure a Service Principal Name (SPN) for Windows Authentication

Use this topic as a checklist to correctly configure the Outlook Add-In so that users can authenticate with EFT using integrated Windows Authentication.

Why do I need an SPN? According to Microsoft Technet, "A service principal name (SPN) is the name by which a Kerberos client uniquely identifies an instance of a service for a given Kerberos target computer. If you install multiple instances of a service on computers throughout a forest, each instance must have its own SPN. A given service instance can have multiple SPNs if there are multiple names that clients might use for authentication. For example, an SPN always includes the name of the host computer on which the service instance is running, so a service instance might register an SPN for each name or alias of its host."

Using the Windows "setspn" utility, create the Service Principal Name (SPN), which is necessary for Kerberos to function correctly for EFT. The SPN is a name by which the Add-In can uniquely identify the EFT Server service.

The “setspn” utility is typically installed by default on Active Directory server computers. The command must be run using an account with Active Directory administration rights. Typically it is easiest to perform these steps on the domain’s primary Active Directory server.

To create the SPNs, execute the following at a command prompt:

```
setspn –A HTTP/eftserver eftpreauthuser

setspn –A HTTP/eftserver.globalscape.local eftpreauthuser

setspn –A HTTP/eftserver.globalscape.com eftpreauthuser
```

Where:

- eftserver eftpreauthuser is the host name of the computer running EFT; the host name that workstations would use internally to communicate with the EFT computer.
- eftserver.globalscape.local eftpreauthuser is the fully qualified host name of the computer running EFT; the full host name that workstations would use internally to communicate with the EFT computer.
- eftpreauthuser with the username of Active Directory domain account used in the “KDC pre-auth username” field of the EFT Kerberos Configuration.
- eftserver.globalscape.com is the address to which the Add-In will connect.

Do not type "HTTP://" -- the proper prefix is "HTTP/"

These SPNs should work regardless of the account the EFT server service is running as.

If duplicate SPNs exist (meaning multiple domain accounts with the same HTTP/<SPN>), then Kerberos will not work correctly. Once the SPN has been associated with the Kerberos Pre-Auth Account used by EFT to participate in Kerberos Authentication, you can double-check for duplicate SPNs on the domain using the command: `setspn –X`.

To view the SPNs to verify that they were created successfully, run the following command after substituting `<PreAuthUsername>`auth user account:

```
setspn –l <PreAuthUsername>
```

(Note: The switch is a lower-cased letter L, ***not*** the number one.)

Configuring Message Options in Outlook

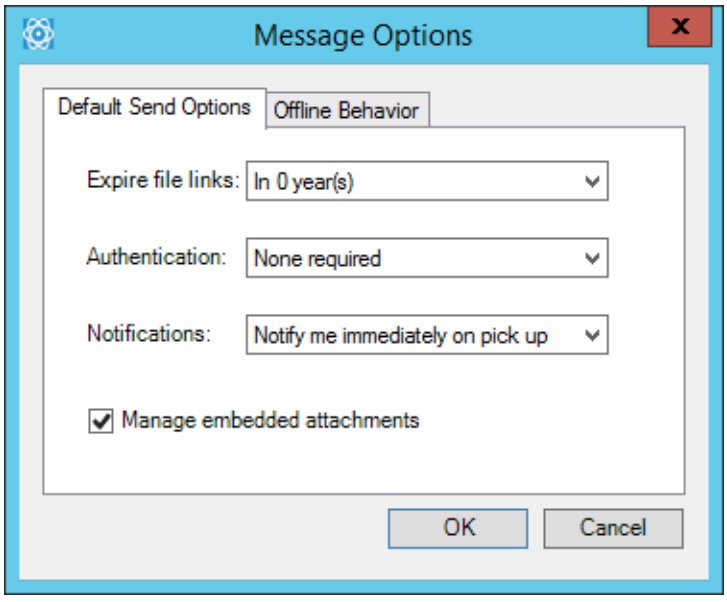
You can configure message options for all emails or for a specific email. In each email that you send, you can specify message options that pertain to that email only, overriding the default send options. You can make these settings stricter, but not less strict. Each procedure is described below.

Use the **Message Options** dialog box to specify whether the EFT Outlook Add-in should:

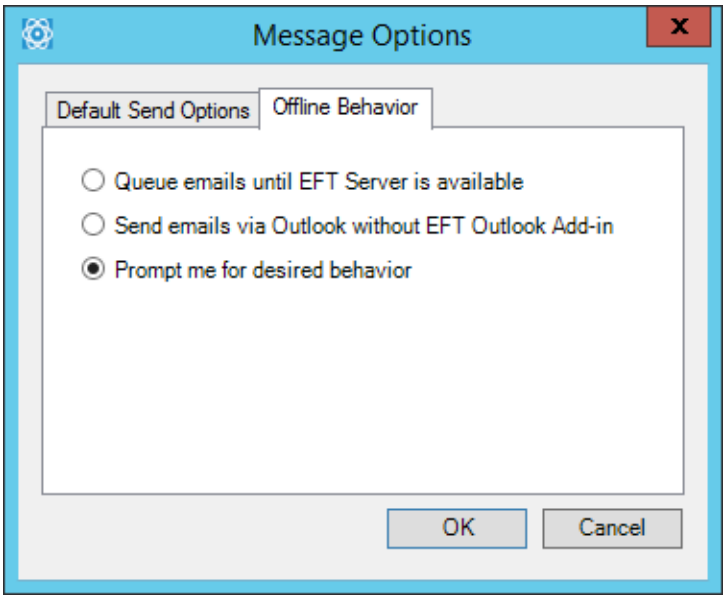
- Expire links
- Use authentication
- Notify on pickup
- Manage embedded attachments
- Queue or send emails when EFT is not available

To configure message options to apply to ALL emails

1. On the EFT Outlook Add-In toolbar/ribbon, click **Message Options**. The **Message Options** dialog box appears.



2. On the **Default Send Options tab**, specify expiration, authentication, and notification options.
3. If you want EFT to manage embedded attachments, such as a signature logo, select the **Manage embedded attachments** check box.
4. On the **Offline behavior**tab, specify the following options:



- **Queue emails until EFT server is available**—Emails are sent after EFT server becomes available.
- **Send emails via Outlook without EFT Outlook Add-in**—Emails are sent immediately, but not managed by EFT.
- **Prompt me for desired behavior**—Display a prompt when EFT is not available so you can choose whether to send immediately or hold the email until EFT is available.

5. Click **OK** to save your changes, or click **Cancel**if you do not want to save your changes.

To configure send options for a specific email

1. Create the email as you normally do.
2. In the EFT Outlook Add-In area, click the options you want to change just for this email.
3. In the **Send Options**dialog box, you can specify the following options:
   - **Offload attachments**—Embedded attachments are files that are inserted into the body of the email rather than attached to the email, such as a company logo in an email signature or a picture. If you want to make these embedded attachments into file download links, select the check box. (Cleared by default.)
   - **Expire File Links**—When selected, the ability to download the attachments will expire in the time that you specify. If the recipient attempts to download a file that is past its expiration date, the following message appears: “The file you are attempting to download has expired. Please

contact the sender if this file needs to be resent." (Cleared by default.)

- If the administrator has selected the Retain files after link expiration check box, the temporary Workspace is removed from the virtual file system in EFT, but the files are still available on disk until the "retain files" expiration date.

- **Authentications**—Require the user to log in to download an attachment from the Pick-up portal. Selecting this check box helps prevent unwanted downloads from email forwarding and such, and also helps guarantee that the person downloading the file is the intended recipient.
  - If the user clicks on an individual file link, the login or account creation page will be displayed in their default browser. After authentication is successful, the "open/save" dialog appears.
  - If the user clicks on the Pick-up portal link, the login or account creation page will be displayed in their default browser. After authentication is successful, they will be taken to the Pick-up page for that specific package.
  - When the check box is selected, only the Pick-Up page link is sent. If the check box is not selected, individual links for each file are included in the email.

  The authentication will be saved in their session, so clicking multiple individual file links will not require multiple log-ins. (The session length is 10 minutes.)

- **Notifications**—When selected, download notification is sent to you when the recipient clicks the download link in the email or Download Files on the Pick-Up page.

4. Click **OK** to save your changes or **Cancel**if you do not want to save your changes.

Enabling or Disabling the Outlook Add-In in Outlook

If the EFT Outlook Add-In options do not appear in Outlook you need to enable it. Or in the rare instance of an error, you may you need to disable the Outlook Add-In or reenable it.

To enable or disable the Outlook Add-In

1. Click **File > Options**.
2. In the left pane, click **Add-Ins**.
3. In the **Manage**box, click **COM Add-Ins**, then click **Go**. The **COM Add-Ins** dialog box appears.
4. Select (turn on) or clear (turn off) the **EFT Outlook Add-In** check box, then click **OK**.

   Take note of the state of the Add-In in the Trust Center (i.e. Active, Inactive, or Disabled). If the Add-In is in a disabled state, it cannot be enabled using the steps above initially. Instead, you must perform the following steps in the Trust Center:

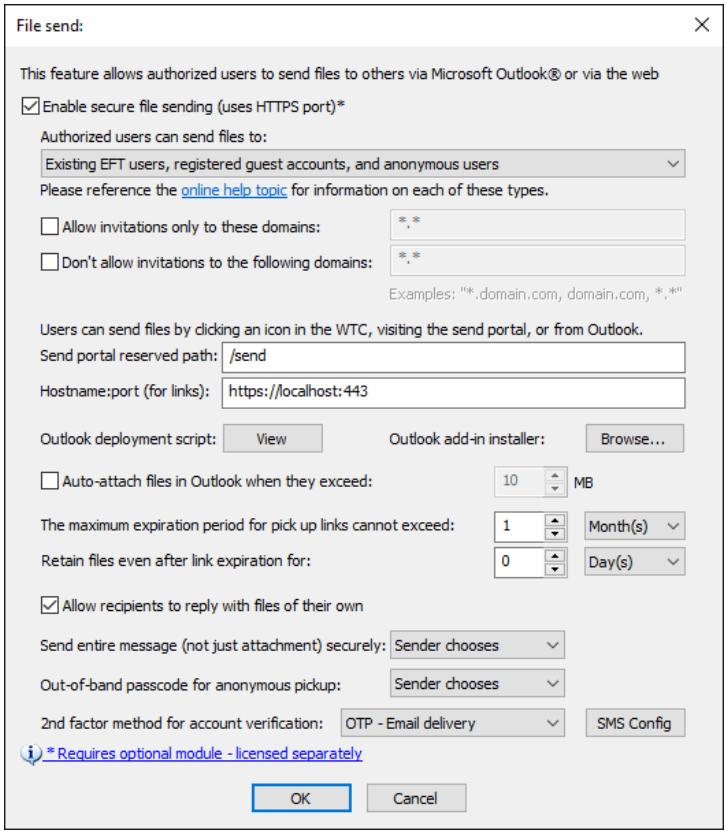
   a. Next to the **Manage**box, click **Disabled Items**, then click **Go**.
   b. In the **Disabled Items**dialog box, click **EFT Outlook Add-In**, then click **Enable**.
   c. Close the **Disabled Items**dialog box.
5. If the Add-In now appears in the Active list, it is enabled. If the Add-In appears in the Inactive list, follow steps 3-4 above.

Deploy Outlook Add-In on End-User's Computers

Configure the Outlook Add-In in the File Send dialog box on the Web tab in the EFT administration interface before deploying the EFT Outlook add-in on end-users' computers.

To deploy the EFT Outlook add-in on end-users' computers

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Site you want to configure.
3. In the right pane, click the **Web**tab.
4. Next to **Send Portal,**click **Configure**. The **File send** dialog box appears.



Do one of the following:

- **Use the EFT Outlook add-in installer.**Click **Browse** to open **C:\Program Files\Globalscape\EFT Server\OAI Installers**, get the EFT Outlook add-in installer, and install the EFT Outlook Add-In as described in Installing the EFT Outlook Add-In. Choose either the EXE or the MSI file. (The EXE will launch the MSI.)
  - **EFTOutlookAddinSetup.exe**will check if Microsoft Outlook is present, install any missing pre-requisites, and then launch the .MSI to install the add-in. When you run the "EXE" make sure the "MSI" file is in the same directory, as the "EXE" launches the "MSI" as part of the install process.
  - **EFTOutlookAddinInstaller.msi**will check if Microsoft Outlook is present, check whether .NET 4.6 is present, and then install the add-in. The "MSI" will not check for or install any missing pre-requisites. It only checks for the presence of Outlook and .NET.

  -OR-

- **Use the Outlook add-in deployment script**.Click **View** to open the **Outlook Add-in Deployment Script**box.
  a. Copy and paste the script into the tool you are using to deploy the Outlook Add-In across your organization.
  b. Click **OK**or press ENTER to close the **Outlook Add-in Deployment Script** box.
  c. Edit the script to match your environment (that is, the EFTHOST IP address and port, username, password).
  d. EFT supports Manual authentication, which is really Basic authentication, so you have to explicitly provide the user's EFT username and password (that is, the username and password that this Add-In user uses to log in to EFT--not the administrator credentials). EFT also supports Integrated Windows Authentication (IWA) where you don't have to explicitly provide a username and password if you are logged into Windows with your domain account.
  e. Edit the Add-In installer command-line arguments depending on the authentication type you want:

     For manual authentication, do the following (EFTUSERNAME and EFTPASSWORD values have to be substituted with the actual Add-in user's EFT username and password):

```
msiexec /lv installation.log /qn /i
EFTOutlookAddinInstaller.msi EFTHOST=https://WIN-
KST875BEBNP EFTPORT=443
EFTAUTHTYPE=MANUAL EFTUSERNAME=username
EFTPASSWORD=test123!
INSTALLLOCATION="%userprofile%\AppData\Roaming\Glo
balSCAPE\EFT Outlook Add-in"
FILESTORELOCATION="%userprofile%\AppData\Local\Glo
balSCAPE\EFT Outlook Add-in"
```

For Integrated Windows authentication, do the following (EFTUSERNAME and EFTPASSWORD don't need to be supplied):

```
msiexec /lv installation.log /qn /i
EFTOutlookAddinInstaller.msi EFTHOST=https://WIN-
KST875BEBNP EFTPORT=443 EFTAUTHTYPE=IWA
INSTALLLOCATION="%userprofile%\AppData\Roaming\Glo
balSCAPE\EFT Outlook Add-in"
FILESTORELOCATION="%userprofile%\AppData\Local\Glo
balSCAPE\EFT Outlook Add-in"
```

Enabling Outlook's Language Detection

The EFT Outlook Add-In uses Outlook's proofing language detection to determine in which language an email is written. If you want to enable the **Auto detect email language**setting, you must enable Outlook's **Detect language automatically**proofing setting.

Before Outlook's **Detect language automatically** option can detect the language that you are typing and enable the proofing tools for that language, you must turn on the language-specific options you want to use.

To turn on language specific options

- For Microsoft Office 2007, refer to the Microsoft Office article at http://office.microsoft.com/en-us/outlook-help/enable-the-use-of-other-languages-in-your-office-programs-HA010243503.aspx.
- For Microsoft Office 2010 and later, refer to the Microsoft Office article at http://office.microsoft.com/en-us/outlook-help/enable-the-use-of-other-languages-in-your-office-programs-HA010354783.aspx.

To enable Outlook's Detect language automaticallyproofing setting

- For Outlook 2007, refer to the Microsoft Office article at http://office.microsoft.com/en-us/outlook-help/turn-on-automatic-language-options-HA010244823.aspx.
- For Outlook 2010 and later, refer to the Microsoft Office article at http://office.microsoft.com/en-us/outlook-help/turn-on-automatic-language-options-HA010354274.aspx.

From the Microsoft Office links above: "Automatic language detection does not work on a single-word basis, but on a sentence basis. Depending on the length of your sentences, you might need to type several sentences before Outlook has enough contextual information to automatically detect the language and apply the correct dictionary."

Outlook must be restarted for the changes to take effect. After you have turned on the language-specific options in Microsoft Office and enabled Outlook's **Detect language automatically** proofing setting, then the Add-In's automatic language detection feature will be enabled.

Mail Profiles with Multiple Accounts

Outlook 2010 and later support mail profiles with multiple mail accounts. The Outlook Add-In seamlessly works with this new feature and (from a user standpoint) there is no real difference in how the Add-In is used. Emails with attachments can be sent from any of the mail accounts in the profile and the Add-In will manage the emails that meet the policy criteria, as usual. If an email is sent with the download notification feature turned on, the notifications will be sent to the account from which the email was sent. The **Status** pane will show an aggregated view of all packages that are being managed by the Add-In for all accounts. If an account is disconnected from its mail server, the Add-In will wait until connectivity is re-established for that account before uploading commences.

The Outlook Add-In is supported with the following mailbox types:

- Outlook 2010 and later support MAPI and POP

Recovering an Email from "Unrecoverable Error"

The Add-In will try to automatically recover from problems such as loss of connectivity with EFT during a transfer. If the Add-In experiences an “Unrecoverable Error” while managing a package, the **Recover Email** button appears. An unrecoverable error is a more serious error that the Add-In cannot resolve on its own, such as a file system error caused by EFT running out of disk space. These types of errors will usually require an administrator to resolve.

If you click **Recover Email**, the Add-In will move the email corresponding to the package from Outlook’s *Outbox* to the *Drafts* folder. You can then try resending the email, perhaps after the administrator has had a chance to resolve the issue. If the problem cannot be resolved in a timely fashion, but you need to send the email promptly, you can stop the Add-In from managing emails by turning it off via the Outlook *Trust Center*.

- To turn off the Outlook Add-In, refer to Enabling or Disabling the Outlook Add-In.
- To edit message options, refer to Configuring Message Options.

Sending Files with the Outlook Add-In

If you have ever sent an email with attachments, you already know how to use the Outlook Add-in. Create the email, attach one or more files to the email, then click **Send**. You will continue to send and receive emails as always; the only difference is that the Outlook Add-in works transparently in the background to transfer the emails that have attachments.

- The sent email is still saved to your **Sent Items** folder, but the attachments, if managed by the Outlook Add-in, are not saved in the **Sent Items** folder. Instead, a link to the attachments is added to the body of the email. The email saved to your **Sent Items** folder looks the same as the recipient's received email, minus the attachments. (Outlook's "Save Sent item to" option is not supported in the EFT Outlook Add-In.)
- The attachment and message, if managed by the Outlook Add-in, is saved on EFT in the location specified during installation, in a unique folder for each email, not on your SMTP server (such as Microsoft Exchange).
- The Outlook Add-in stores information about emails that it is processing in an individual workspace.
- The administrator configures message-sending options on EFT. You can configure more strict options in Outlook for all messages or for specific messages. Refer to Configuring Message Options for details.
- You can send a secure message in Outlook without an attachment, however, you cannot expire the message immediately without an attachment.

Sending the email can fail in the following situations:

- **Offline mode**—Messages are stored in the outbox until Outlook is online and the Add-In connects to the server.
- **Loss of connectivity to the server**—Interrupted uploads due to loss of connectivity to the server are continued from the point at which they were stopped when connection to the server is re-established.
- **Insufficient disk space**—The Add-In will receive a FileSystemError response from the server and the Add-In will treat this as an unrecoverable error.
- **RTF-formatted emails**—RTF-formatted messages are not supported. To change the format for all messages sent in Outlook, refer to Changing the Message Format.

To send a file

1. Create an email in Outlook as you normally do.
2. Attach the file to the email using the EFT Outlook Add-in **Offload Attachments** button.
3. (Optional) Click one or more of the following options:
    - **Secure Message**—To send the email and its attachments as a secure message, click **Secure Message**. The attachment(s) and message body will be available to the recipient(s), through a secure Pick-Up portal. A unique message containing a unique link is created for each recipient. When processing a message in Outlook, if **Secure Message** is set (by user or mandatory), then that message will be processed by EFT, including any files (if any) that are attached.
    - **Expire File Links**—When selected, the ability to download the attachments will expire in the time that you specify. If the recipient attempts to download a file that is past its expiration date, the following message appears: “The file you are attempting to download has expired. Please contact the sender if this file needs to be resent.”
        - If you set the message to expire immediately without attaching a file, you will receive an error message.
        - If the administrator has selected the Retain files after link expiration check box, the temporary Workspace is removed from the virtual file system in EFT, but the files are still available on disk until the "retain files" expiration date.
    - **Authentications**—Require the user to log in to download an attachment from thePick-up portal. Selecting this check box helps prevent unwanted downloads from email forwarding and such, and also helps guarantee that the person downloading the file is the intended recipient.
        - If the user clicks on an individual file link, the login or account creation page will be displayed in their default browser. After authentication is successful, the "open/save" dialog appears.
        - If the user clicks on the Pick-up portal link, the login or account creation page will be displayed in their default browser. After authentication is successful, they will be taken to the Pick-up page for that specific package.
        - When the check box is selected, only the Pick-Up page link is sent. If the check box is not selected, individual links for each file are included in the email.

The authentication will be saved in their session, so clicking multiple individual file links will not require multiple log-ins. (The session length is 10 minutes.)

- **Notifications**—When selected, download notification is sent to you when the recipient clicks the download link in the email or "Download Files" in the Pick-Up portal.

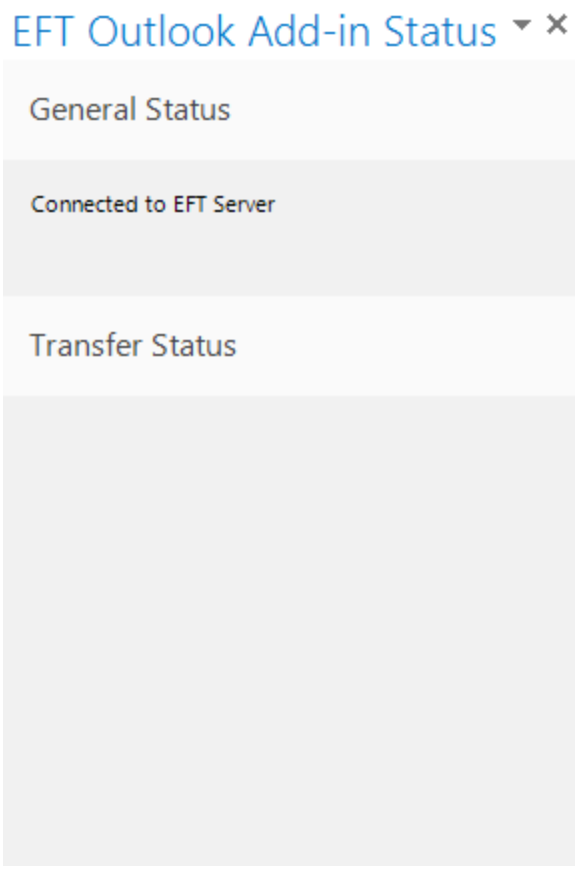
4. Click **Send**. The email the recipient will receive a delivery notification.
5. The recipient can download the attachment from the Web Transfer Client.
6. If the attachment does not appear, the recipient might need to click the refresh icon. Select the check box next to the file, then click the **Download** icon. The file is saved to the downloads folder in the recipient's browser.

Viewing Add-In Status

The EFT Outlook Add-In includes a **Status**pane through which you can view whether you are connected to EFT and the status of email attachments being sent. By default, the **Status**pane is hidden. The pane appears on the right side of the main Outlook window.

To view EFT Outlook Add-in status

- On the **EFT Outlook Add-In** toolbar/ribbon, click **Display Status**. The **EFT Outlook Add-in Status** pane appears.



  - The **General Status**area displays the status of your server connection. If the Outlook Add-In is not connected to the server, it will not try to upload packages.
  - The **Transfer Status** area displays the status of attachments being sent, including recipient, subject line, size of the file, status (Pending, Transferring, Verifying File Digest, etc.), and the number of upload attempts.

- To dock or undock the **Status**pane
  - Click and hold the title bar of the **Status** pane until the **Move** cursor appears (or click the down arrow on the title bar of the pane, then click **Move**) then drag the pane to undock it and move it where you want.
  - To dock the pane, click in the title bar, and drag the pane back to the right or left side of the primary Outlook window.
  - To resize the pane (when undocked) click and hold a corner of the pane (or click the down arrow on the title bar of the pane, then click **Size**), then drag the pane to the size you want.
- If the upload failed, the **Transfer Status** area displays the following information:
  - Text-based description of current status, including information on what prevented package from being uploaded in error cases
  - Subject of the package
  - Recipients of the package
  - Total size of package
  - Number of upload retry attempts for package
  - Recover Email button for failures that were the result of an unrecoverable error. Clicking **Recover Email**moves the email to the Outlook **Drafts**folder.

Mobile Transfer Client (MTC)

The topics below describe the Mobile Transfer Client (MTC) features and how to use it to access files on EFT using a mobile device.

- MTC Introduction and Features
- Enabling and Configuring the MTC
- Obtaining the Mobile Transfer Client Apps

Mobile Transfer Client Introduction

The Globalscape MTC v1 is designed to work exclusively with Globalscape's managed file transfer solution known as EFT. With the Globalscape MTC, organizations can provide employees, partners, and customers with access to corporate data from their mobile devices, while keeping the data safe and secure within the organizational boundaries.

Download the Globalscape MTC application from https://play.google.com/store/apps/developer?id=HelpSystems.

The Mobile Transfer Client (MTC) supports the following features:

Security

- Secure communications and transport over HTTPS
- SSL certificate management (accept CA-signed certificates, otherwise prompt)
- Secure data storage
- Central policy management that controls:
    - Profile password storage
    - Data caching
    - Storing data in an offline repository (vault)
    - Sharing files via email
    - Opening files in external (third-party) apps

Profile Management

- Multiple profile support
- Single "tap-on" link for automatic profile provisioning
- Dual-stack (IPv4 and IPv6) support
- International Domain Name (IDN) and Punycode support
- Support for non-default ports
- Auto-login to last connected profile on app launch
- Password reset and recover lost username support
    - Password reset must be done in the WTC. If "Force users to change their password immediately upon next use" is selected on the **Security** tab, be sure to inform MTC users to log in to the WTC before using the MTC.
- Full support for Unicode characters
- Support for 64-bit devices

Files Listings and Transfers

- View up to 10,000 files in a directory listing
- Transfer files up to 3GB in size
- Transfer multiple files concurrently
- Pause and resume transfers
- Automatic resume of system paused transfers
- Resume partial transfers from point of failure
- Download files to a separate secure repository for offline access
- Download files and open them using the built-in file viewer (Only certain file types are supported.)
- Open text, log, and other ASCII files in the internal text viewer
- Download files then open in an external program
- Download files and share them as email attachments
- Download files, make edits, then upload the modified version
- Automatic and transparent file integrity checking
- Create, rename, and delete folders
- View download progress
- Abort transfers and retry failed transfers

General Settings and Logs

- Clear profile and vault caches
- Specify the maximum cache size
- Enable logging, including verbose logging
- View detailed transaction logs
- Email logs to your administrator
- Clear all logs
- Disallow password saving (global option)
- Custom/branded profile icons (optional)
- Chose light or dark theme

Enabling and Configuring the Mobile Transfer Client in EFT

Perhaps the most important feature available to the MTC, aside from an always secure connection, is the centrally managed security controls that dictate what users can and cannot do within the MTC app when connected to EFT.

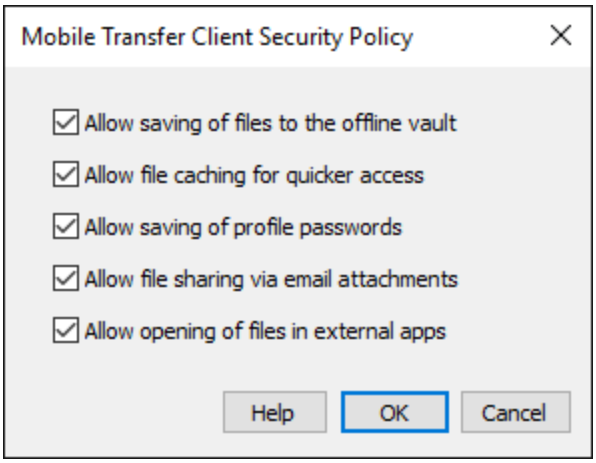
Server and Site administrators can also block MTC connections, effectively terminating the connection based on the user-agent string that identifies the client as an MTC client. (This does not prevent other file transfer clients—mobile or desktop—from connecting to EFT.)

MTC's security policy only applies to files in the remote directory. The security policy does not apply to files in the vault, which means that any file downloaded to the vault can be shared or opened in third-party applications. If the EFT administrator doesn't want users to share files or open them in third-party apps, then EFT should be configured to not allow users to save files to device's vault.

MTC is configured at the Site level for all Settings Templates and users.

To enable the MTC in EFT and configure security controls

1. In the administration interface, connect to EFT and click the **Server**tab.
2. On the **Server**tab, click the Site that you want to configure.
3. In the right pane, click the **Connections**tab.
4. If not already enabled, enable HTTPS and create and assign an SSL certificate for the Site.
5. Select the **Allow Globalscape Mobile Transfer Client (MTC) over HTTPS** check box.
6. Click **Configure**. The **Mobile Transfer Client Security Policy** dialog box appears.



7. Each time a user connects or makes specific requests to MTC, their profile is updated with the latest security control settings. Select (enable) or clear (disable) the following check boxes:
    - **Allow saving of files to the offline vault**—The vault in the MTC app is an encrypted storage area* where a user can download a *copy* of a remote file (from this or possibly another EFT account) for subsequent access, even when offline, and even if the user no longer has an account on EFT. If you disable the ability to store files in the vault then you should alsoconsider disabling **Allow file sharing via email attachments**and **Allow opening of file in external apps**, since in all three instances files essentially leave your control.
    - **Allow file caching for quicker access**—The cache is an account (MTC profile)-specific secure storage area* that MTC uses to keep copies of files that were downloaded. The next time a user taps on a file (to open in the internal PDF viewer, for example), the file will be opened from the device's cache (assuming it isn't stale data) rather than downloaded again from the server, resulting in a better end-user experience. The cache is semi-permanent in that it will grow as files are downloaded, and is not cleaned up unless space is needed or the user decides to clear the local cache (similar to how a browser's cache works). Disabling this option doesn't disable file caching altogether, but rather makes caching temporary, cleaning up cached data upon application exit.
    - **Allow saving of profile passwords**—Preventing the user from saving the password forces them to re-type it each time they connect to EFT. Once authenticated, the app will retain the password in memory until the app is exited. If this setting is disabled in EFT, the password field appears dimmed in the MTC app (for this profile) and passwords for this profile are removed from the mobile keychain (iOS) or database (Android), if stored there. If this setting is enabled, then it is up to the user to decide whether to store the password in the MTC app.

- **Allow file sharing via email attachments**—After downloading a file, an MTC user can optionally share the file as an email attachment with another user (taking the file outside of MTC's control). If this setting is disabled in EFT, then sharing won't be allowed from within the MTC application. If you disable the ability to share files, then you should also consider disabling **Allow opening of file in external apps** and **Allow saving of files to the offline vault**, since in all three instances files essentially leave your control.
- **Allow opening of file in external apps**—After downloading a file, an MTC user can optionally open the file in a third-party app, which is often necessary if there is no internal MTC viewer that can open the particular file extension.
  When the user performs an "Open In" operation, the file is decrypted so that the external app can accept the file (which is now outside of MTC's control). This setting provides administrators the ability to block users from opening files in other apps, forcing them to use the in-app viewer (if available) or nothing at all. If you disable the ability to open files, then you should also consider disabling **Allow file sharing via email attachments** and **Allow saving of files to the offline vault**, since in all three instances files essentially leave your control.
- *Read the section on data encryption in the MTC FAQ. Files saved to disk on Android are not sandboxed, as in iOS, thus minimizing the effectiveness of some of the above controls. However, MTC does leverage Android's "Internal Storage" for keeping it segmented and inaccessible to other apps, at the cost of much less available disk space than if the standard physical storage had been used, which is "world shareable" and thus unsuitable for storing corporate data, even if device encryption is enabled. (The third-party app cannot arbitrarily do so; the user must perform an "Open" operation from the other app and select the file located elsewhere in the data folder.)

8. Click **Apply**to save the changes on EFT.

To disable or block MTC

- Clear the **Allow Globalscape Mobile Transfer Client (MTC) over HTTPS** check box or disable HTTPS.

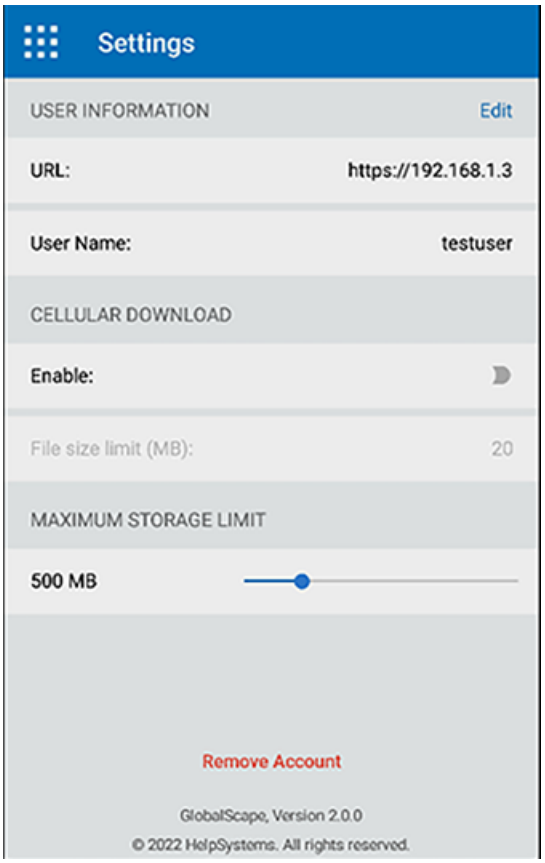
Related Topics

- Enable or Disable HTTPS
- Connect to EFT
- Enable HTTPS

- Create a certificate
- Assign an SSL certificate to the Site

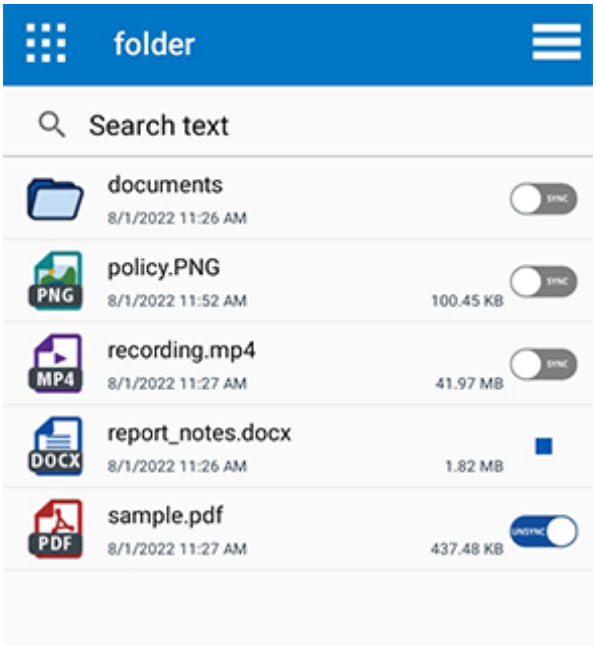
Create a Profile

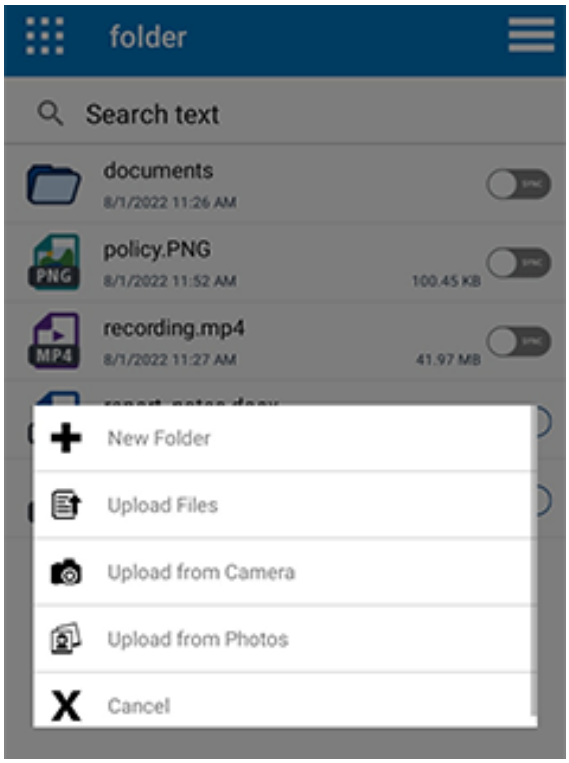
The Mobile Transfer Client is designed to connect to Globalscape EFT. Before you can use the app, your administrator will need to create an EFT account for you and provide you with your account details. Once your account is created and enabled in EFT, you will receive a special link in your email that, when tapped on your device, will auto-provision MTC with your account profile details. Alternatively, you will receive your login credentials, including the EFT host address, your username, and your password, which you can enter manually.



Connecting to EFT

After you have defined a profile in MTC, tap on the profile to connect. The files and folders in your home directory will appear. Depending on the permissions defined for your account in EFT, you can upload, download, rename, delete, and create folders.





- If you try to navigate into a folder that no longer exists on the server, you are thrown back to the root folder, and message is displayed about inability to perform the action.
- Depending on the security policies defined in EFT, you will be able to preview files, open files in an external application, add files to an offline vault, and share files as attachments.
- The default settings are fine for most users. If you want to change any settings, the **Settings** screen of the MTC app allows you to view storage limits, clear profile cache and vault, manage logging, specify whether to save profile passwords, and whether to clear the profile's long -term cache automatically or manually. You can also see which version of the app is installed, displayed at the bottom of the page.
- Logging can be used by support to troubleshoot any problems with the MTC app. **Log operations**, **Log communications**, and **Purge logs on app exit** are turned off by default. If you have had logging turned on and no longer need it, you should turn off logging so as not to take up storage space. Tap **Purge logs now** when the logs are no longer needed.
- If your password has changed, no requests to the server will be allowed from the client until you log out and log back in with the new password.

Obtaining the Mobile Transfer Client App

The Mobile Transfer Client (MTC) is available for Android devices as an app, also called a native app (as opposed to a browser-based app).

To download the app onto a device

- Go to the Google Play store on your device, and search the app store for "Globalscape MTC" The links to the MTC app are also included in the credentials template email.

DMZ Gateway

The DMZ Gateway® server is designed to reside in the demilitarized zone and provide secure communication with EFT behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ.

The topics below describe how install and administer DMZ Gateway.

- Introduction to DMZ Gateway
- What's New in DMZ Gateway
- System Requirements for DMZ Gateway
- Enabling DMZ Gateway in EFT
- DMZ Gateway Technical FAQ
- DMZ Gateway Knowledgebase Articles
- Installing DMZ Gateway
- Administering DMZ Gateway
- DMZ Gateway Secure PNC
- Interface Reference

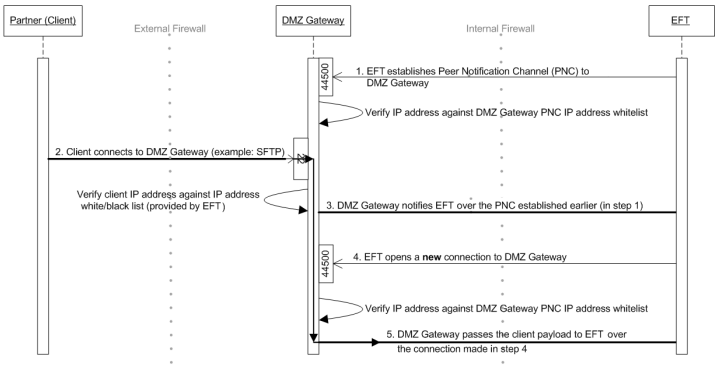
Introduction to DMZ Gateway®

DMZ Gateway®is used in combination with EFT to create a multitier security solution for data storage and retrieval. The DMZ Gateway resides in the demilitarized zone to provide secure communication with EFT behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ, and with no sensitive data stored in the DMZ, even temporarily. DMZ Gateway supports connections to EFT using Profiles. Depending on the license purchased, you can have up to 15 Profiles (unique IP address:port connections).

How Does It Work?

1. When the EFT service is started, it will establish (and maintain) an outbound connection to the DMZ Gateway. This proprietary, non-encrypted connection is called the Peer Notification Channel (PNC). EFT and DMZ Gateway use the PNC to setup subsequent communications between EFT and incoming client connections.
2. When a client (web browser, FTP client, etc.) connects to DMZ Gateway on a pre-approved port (21, 22, 80 443, etc.), DMZ Gateway will cross reference the client's IP with the IP access list (provided by EFT over the PNC) before proceeding any further.
3. If the IP is accepted, DMZ Gateway will notify EFT over the PNC of the new client connection, providing data such as the client's IP address and the port to which they are connected.
4. EFT will subsequently create a new outbound connection to the DMZ Gateway to the same port that is being used by the PNC for associating with the client connection made in step 2.
5. DMZ Gateway will then proceed to read the inbound payload data from the client and send the payload data to EFT for processing. DMZ Gateway will also read any outbound data communication from EFT and send it to the client.

The graphic below describes the flow in EFT:



What's New in DMZ Gateway®?

Below are the changes to DMZ Gateway. Complete release notes are available in the Globalscape support portal as well as the Fortra release notes portal:

DMZ Gateway Release Notes (Globalscape Client Success Portal)

DMZ Gateway Release Notes (Fortra Portal)

Changes in DMZ Gateway version 4.0

- **New Features**
  - Updated DMZ Gateway interface to Fortra branding
  - Automatically sign Admin Launcher during installation
- **Enhancements**
  - Verified support on latest operating systems
  - Updated default list of cipher suites
  - Updated Java to latest version of OpenJDK
  - Updated Apache libraries
  - Updated license for service wrapper

Changes in DMZ Gateway version 3.5.0.35

- Released 3/17/2022
- Updated Log4j to v2.17 (which also updated logging parameters) (TFS 383247)
- Updated DMZ graphics to include HelpSystems branding (TFS 383503)

Changes in DMZ Gateway version 3.5.0.23

- Released 3/17/2020
- Updated MTP SDK version 4.3.0-Passive
- Extended Accelerate module trial to August 2020 (available in EFT prior to v8.0.5.7)

Changes in DMZ Gateway version 3.5.0.21

- Released 2/13/2020
- Updated JDK to 8u202

Changes in DMZ Gateway version 3.5.0.16

- Released 6/13/2019
- Updated Accelerate module to 1.0.0.30, extended trial to October 2019 (available in EFT prior to v8.0.5.7)

Changes in DMZ Gateway version 3.5.0.14

- Released 1/31/2019
- Updated Accelerate module to 1.0.0.27, extended trial to April 2019 (available in EFT prior to v8.0.5.7)
- Updated Copyright year

Changes in DMZ Gateway version 3.5.0.12

- Released 9/27/2018
- Updated Accelerate module to 1.0.0.24, extended trial to January 2019 (available in EFT prior to v8.0.5.7)
- Fixed an issue where DMZ Gateway PNC help section had broken links

Changes in DMZ Gateway version 3.5.0.11

- Released 5/14/2018
- Extended Accelerate module trial to June 2018 (available in EFT prior to v8.0.5.7)
- Updated splash screens
- Added support for Secure PNC with EFT

Changes in version 3.4:

- Released April 25, 2016
- EFT version 7.3.0 and later (Windows OS only)
- Support for EFT with the Accelerate module (available in EFT Enterprise prior to v8.0.5.7)

  The Accelerate module/FAST protocol is not supported on Linux versions of DMZ Gateway.

Changes in version 3.3.1:

- Released December 8, 2014
- EFT v6.5 and later
- Removed support for Windows Server 2003
- Added Business Activity Monitor (BAM) as a recognized server type

- Upgraded the Java Service Wrapper to Version 3.5.19. This version includes an automatic deadlock detection/restart feature.

Changes in version 3.3.0:

- Released February 15, 2013
- EFT v6.5 and later
- Support for IPv6 addressing when operating with Mail Express version 3.3 and later
- Added support for Unicode strings in the log files and XML-based configuration files
- Added support for Unicode strings in communications with the EFT platform v6.5 and later
- Changed installer so that it now ensures the DMZ Gateway administration interface is not running prior to making modifications
- Fixed an issue that prevented binding to interfaces if IPv4 or IPv6 support was disabled in the operating system
- Fixed minor user interface issues in the DMZ Gateway administration interface
- Upgraded the embedded Java Runtime Environment to version 1.7.0_09.

Changes in version 3.2:

- Released December 7, 2011
- EFT v6.4 and later
- Support for IPv6
- Added minor usability features in the administration interface
- Added minor usability features in the Windows installers
- Upgraded various third-party libraries to most recent versions
- Upgraded the embedded Java Runtime Environment to version 1.7.0.

Changes in version 3.1:

- Released March 22, 2011
- EFT v6.3
- Support IP Access Rule functionality
- Can connect to Mail Express v3.1 and later
- Works with v6.4 if you are ***not***using IPv6

Changes in version 3:

- Released March 1, 2010
- EFT v6.2.x

- DMZ Gateway's interface was completely redesigned (from v2.x line) to accommodate multiple profiles and extended communication information
- Can be installed not only on Windows, but also on RedHat, SuSE Linux, and Solaris, on 32-Bit or 64-Bit operating systems (For a list of supported operating systems, refer to System Requirements for DMZ Gateway.)
- Can connect to up to 15 EFT Sites simultaneously
- IP address access policy changes are now automatically propagated to DMZ Gateway when the policy is modified in EFT whether in the EFT interface or by the auto-ban logic
- Moved DMZ Gateway licensing to the server to simplify DMZ Gateway installation and activation
- Loggingwas improved and expanded
- Hardened to better withstand attacks from several Denial of Service (DoS) attack tools

System Requirements for DMZ Gateway

It is possible for DMZ Gateway to function with other operating systems, software, and hardware, but has only been tested with the systems listed below.

EFT and DMZ Gateway can**not**be installed on the same computer/image, but must be installed no more than one network “hop” away with an average network latency no greater than 50ms, with zero percent packet loss, and normal packet flow. Refer to the KB article Can I use EFT and DMZ Gateway on separate networks, remote from each other, across a WAN?for more information.

The Accelerate module/FAST protocol (deprecated) is **not** supported on Linux versions of DMZ Gateway, and **not** on EFT v8.0.5.7 or later.

- Supported operating systems:
  - Windows Server 2022

    Windows Server 2019
- 2 CPUs
- 200 MB hard drive space for the application (No data is ever stored on the DMZ Gateway computer, not even temporarily.)
- 1GB available RAM
- 1280x800 resolution or higher display (headless computer supported on non-Windows systems)
- The installer uses the last "free" version of the Java Runtime Environment. If you want to upgrade to the latest version, you need to purchase a license from Oracle. Refer to Knowledgebase article Updating the Oracle JRE for DMZ Gateway for more information.
- Remote administration must be available.
- DMZ Gateway v3.5 and later is supported only on EFT v7.4 and later.

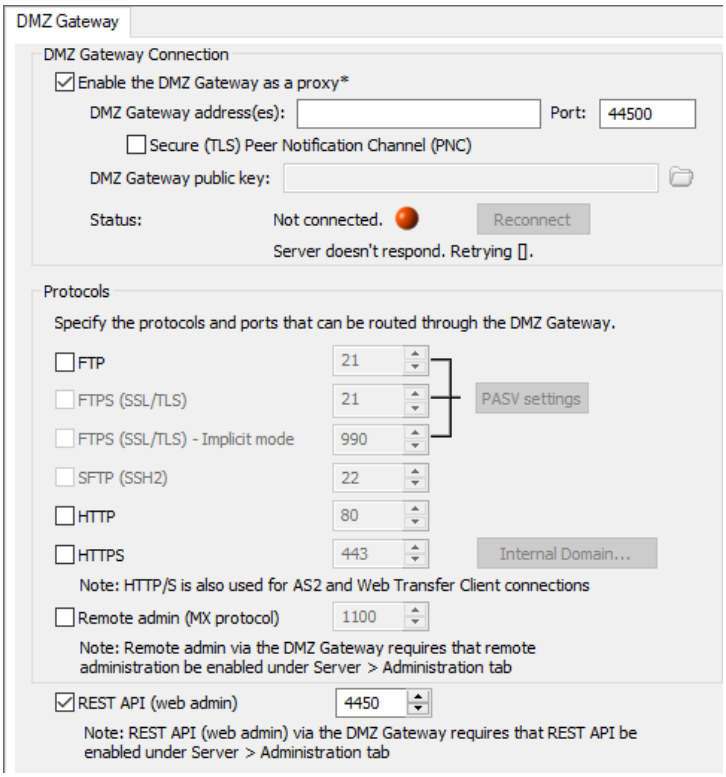
DMZ Gateway Tab - Configuring Perimeter Network Security

After you have installed the DMZ Gateway module, configure the EFT connection to DMZ Gateway. You can enable DMZ Gateway when you create the Site or enable it later in the EFT administration interface. In the Site Setup wizard for both standard and high security-enabled Sites, EFT displays the **Perimeter Security** configuration page that asks whether you will be using DMZ Gateway, and allows you to enter the DMZ Gateway IP address and port number. If **Connect this site to EFT's DMZ Gateway** is selected when you are creating a Site in the Site Setup wizard, EFT attempts to establish a socket connection to DMZ Gateway when you click **Next**.

- If the socket connection fails, a message appears in which you are allowed to provide the DMZ Gateway information again or disable DMZ Gateway and continue without it. (You can attempt to configure it again later.)
- If the socket connection is successful, EFT applies the settings and continues with Site setup.

To enable DMZ Gateway in EFT

1. In the EFT administration interface, connect to EFT and click the **Server** tab.
2. Click the node of the Site you want to connect to DMZ Gateway, then click the **Gateway** node.
3. In the right pane, the **DMZ Gateway** tab appears.



4. Select the **Enable the DMZ Gateway as a proxy**check box.
5. Specify the IP address and the port number of the DMZ Gateway to which you are connecting. The default port is 44500. The connection will be refused if the port is being used by another DMZ Gateway/ Site or if the IP address is on the IP address ban list.)
6. Select the **Secure (TLS) Peer Notification Channel (PNC)** check box. (Refer to DMZ Gateway Secure PNC for more information.)
7. In the **Protocols** area, select the check boxes for the protocols and the external listening ports that DMZ Gateway will use. You can only choose FTP, FTPS, or SFTP if it is enabled on the Site. This is a separate configuration from the ports that EFT uses. For example, you could use port 21 for FTP traffic for EFT, but port 14421 for FTP traffic through the DMZ Gateway.

   > **NOTE:** Refer to Remote Administration through DMZ Gateway for information about remote administration with the MX protocol.

8. If you are using DMZ Gateway with a PASV mode IP address, click **PASV settings**. The **Firewall/NAT Routing** dialog box appears.
   a. Select the **Assign PASV mode IP address**check box, then specify the IP address and port range.
   b. Click **OK**.
9. Click **Apply** to save the changes on EFT.

10. Establish a new connection with EFT by stopping and restarting connected Sites.
    a. On the **Server**tab, click the Site node.
    b. In the right pane, click the **General** tab.
    c. Click **Stop**. The **Site Status** area displays "Stopped" with a red ball icon.
    d. Click **Start**. The **Site Status** area displays "Running" with a green ball icon.

Acceleration

Refer to the knowledgebase article "EFT Accelerate Module" for information about configuring the Accelerated transfers on the DMZ Gateway tab.

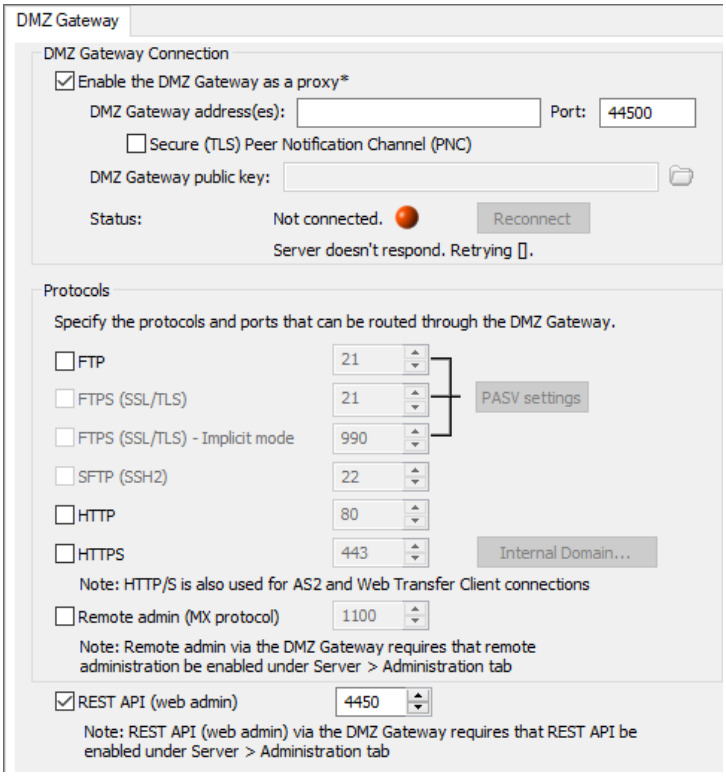
DMZ Gateway in EFT

You can enable DMZ Gateway when you create the Site or enable it later in the EFT administration interface. In the Site Setup wizard, EFT displays the **Perimeter Security** configuration page that asks whether you will be using DMZ Gateway, and allows you to enter the DMZ Gateway IP address and port number. If **Connect this site to EFT's DMZ Gateway** is selected when you are creating a Site in the Site Setup wizard, EFT attempts to establish a socket connection to DMZ Gateway when you click **Next**.

- If the socket connection fails, a message appears in which you are allowed to provide the DMZ Gateway information again or disable DMZ Gateway and continue without it. (You can attempt to configure it again later.)
- If the socket connection is successful, EFT applies the settings and continues with Site setup.

To enable DMZ Gateway in EFT administration interface

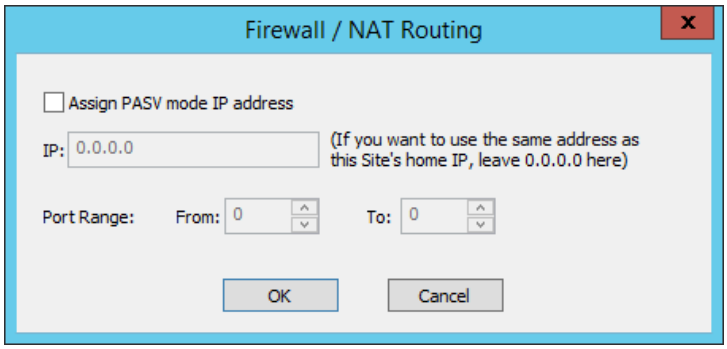
1. In the EFT administration interface, connect to EFT and click the **Server** tab.
2. Expand the node of the Site you want to connect to DMZ Gateway, then click the **Gateway** node.
3. In the right pane, the **DMZ Gateway** tab appears.



4. Select the **Enable the DMZ Gateway as a proxy**check box.

5. In the **DMZ Gateway addresses** box, specify one or more IP addresses of DMZ Gateways to which you are connecting.
    - For multiple DMZ Gateways, specify the addresses separated by commas. EFT will try one IP address, then the next, until it can connect (using the same values, keys, etc. for each one).
    - If DMZ Gateway has previously connected and then the connection is lost, after a 1-second delay, it will try to reconnect, then failover to the next address in the list, then the next, until it connects. (Depending on the "gw_retryattempts" advanced property.) If it fails the last address in the list, it will not try again; EFT server service restart is required.
    - Upon EFT server service restart, it will try again to connect to the first address in the list, and so on.
6. In the **Port** box, specify the port number over which EFT is to connect to DMZ Gateway. The default port is 44500.

    The connection will be refused if the IP address is on the server's IP Access\Ban list.
7. Select the **Secure (TLS) Peer Notification Channel (PNC)** check box.
8. In the **Protocols** area, select the check boxes for the protocols and the ports that DMZ Gateway will use. These settings are separate from the ports that EFT uses. For example, you could use port 21 for FTP traffic directly to EFT, but port 14421 for FTP traffic through the DMZ Gateway.
9. If you are using FTP and DMZ Gateway with a PASV mode IP address, click **PASV settings**. The **Firewall/NAT Routing**dialog box appears.



    a. Select the **Assign PASV mode IP address**check box, then specify the IP address and port range.
    b. Click **OK**.
10. If you plan to use REST API via DMZ Gateway for the Web Admin, select the **REST API (web admin)** check box and specify the port to use. (REST API must also be enabled on the **Administration** tab of the EFT server.)

11. Click **Apply** to save the changes on EFT. If the settings are correct and the DMZ Gateway is configured properly, the connection status changes to **Connected** with a green icon.

    If EFT cannot connect to DMZ Gateway, ensure that the EFT computer can connect to the DMZ Gateway computer by pinging it. Verify that the DMZ Gateway computer's firewall is not blocking incoming connections.

12. You may need to establish a new connection with EFT Server by stopping and restarting connected Sites.
    a. In the left pane, click the Site node.
    b. In the right pane, click the **General** tab.
    c. Click **Stop**. The **Site Status** area displays "Stopped" with a red ball icon.
    d. Click **Start**. The **Site Status** area displays "Running" with a green ball icon.

Related Topic

- DMZ Gateway Secure PNC(Remote administration)

DMZ Gateway Technical FAQ

Below are some frequently asked technical questions about the DMZ Gateway.

Does DMZ Gateway modify the client's packets?

DMZ Gateway effectively terminates the client's TCP/IP session at the DMZ Gateway. The client data contained within the payload of the TCP/IP packet is transmitted to the server over the independently established TCP/IP connection between the server and DMZ Gateway. No modifications are required or performed on the actual payload data, but rather the payload is sent as is to the server. Thus, if the client is using HTTPS, then the HTTPS payload is streamed on through to the server. Unlike a network hardware bridge/router device, the DMZ Gateway does not "pass through" modified packets by changing the TCP/IP or frame layer headers. Instead, the DMZ Gateway reads in a buffer full of data from the client TCP/IP stream (~64KB) and then sends that data over the TCP/IP socket established earlier by the server (see step 4 above). The result is a set of completely different TCP/IP packets with different source and destination locations but containing the original payload. Keep in mind that the original (source) location (IP address) is known by the server as it was provided to the server earlier by DMZ Gateway (see step 3 in Enabling DMZ Gateway in EFT).

Does DMZ Gateway forward client connections to the server?

The DMZ Gateway does not forward client connections. Only the payload (data) is forwarded or passed through to the server.

How do the server's listening ports affect DMZ Gateway?

EFT allows you to define two groups or sets of listening ports. When used with DMZ Gateway, the external listening ports (DMZ Gateway Internet facing) are specified in EFT Server's administration interface on the DMZ Gateway tab. EFT's second set of listening ports, defined on the Site's **Connections**tab, are ONLY used for establishing internal listening ports (server-network facing) for each supported (and enabled) protocol. These sets of ports can be the same or different (even for the same protocol). When DMZ Gateway is NOT being used (that is, the server is residing in the DMZ or is being used for internal, network-facing transactions), then only a single set of ports is used, defined on the Site's **Connections**tab, for all incoming connections to EFT.

How is the PNC created and maintained?

Once configured to work with DMZ Gateway, the server (when running) will always attempt to initiate, maintain, and, if necessary, reconnect to DMZ Gateway's PNC port. No further administrative action is required in the server to establish or maintain communication after the initial setup. From DMZ Gateway's perspective, if the PNC

channel is broken, DMZ Gateway will refuse new (and existing) client connections until the server re-establishes a connection.

The server will “ping” the DMZ Gateway every 5 minutes. If a reply is not received within 10 seconds, the server considers the connection lost, severs the current connection, and then attempts to reconnect. DMZ Gateway also maintains its own awareness (ping/pong) of whether the server is connected. Every 30 seconds, DMZ Gateway determines whether it has received a pong message from the server since the last ping. If it has, it will ping again; if not, it drops the connection. This test allows it to free up ports if the server is not available (that is, no longer responds to ping) and for error reporting. (Refer to the Knowledge Base article "How do EFT and DMZ Gateway Server communicate with each other?" for information about changing these defaults.)

The PNC between the server and DMZ Gateway is not encrypted; however, the external client’s encrypted session will be streamed all the way through to the server, so only the intercommunications between the server and the DMZ Gateway are in the clear, not the client session (assuming they used a secure protocol such as SFTP or HTTPS). (Refer to DMZ Gateway Secure PNCfor information about configuring a secure PNC.)

But won’t an insecure PNC be vulnerable to a man-in-the-middle attack?

In order to usurp the PNC connection, the attacker would need full control over the internal systems on which the server is running. This access would indicate a far greater threat to Confidentiality, Integrity, and Availability (CIA) already in place in your network. Keep in mind that the internal firewall should be configured to allow only outbound connections from the server to DMZ Gateway via the PNC port. If configured as such, then the ability to usurp the control connection doesn’t really gain the attacker much of an edge. Even if a connection were seized, the attacker would need to perform several other non-trivial steps, such as spoofing the server’s IP address*, reverse engineering the protocol, opening ports on the firewall, altering the routing table, etc.

*DMZ Gateway provides an optional whitelist for IP addresses that are allowed to connect to the PNC port. (Refer to DMZ Gateway Secure PNCfor information about configuring a secure PNC.)

Isn’t DMZ Gateway just giving users a way to bypass the firewall without providing any security functionality or filtering?

The DMZ Gateway is not designed to replace firewalls or content-inspection devices. The DMZ Gateway’s main purpose is to allow network administrators to minimize the exposure surface area by allowing you to further lock down the internal firewall such that only outbound connections are needed, thus eliminating the need for inbound connections through your internal firewall to your directory server (for user authentication) or SQL/Oracle server (for transaction auditing). Furthermore, it eliminates the need to store file data in the DMZ. Essentially DMZ Gateway limits the attack vector to the server as opposed to multiple other internal servers. As far as

filtering is concerned, it is important to note that DMZ Gateway does not replace any other sort of filtering mechanism, such as firewalls, web application firewalls, content inspection devices, and so on. DMZ Gateway is intended to work with and extend existing security mechanisms.

So then, any vulnerability in the server is essentially exposed to the Internet?

Assuming vulnerabilities exist then yes, those would be exposed to the Internet; however, the attack vector would be limited to attacks that could be accomplished over the network protocols that are proxied through the DMZ, as there would be no means for the attacker to establish inbound connections to the server directly, because of the EFT <> DMZ Gateway architecture. (Refer to DMZ Gateway Secure PNC for information about configuring a secure PNC.)

What about Denial of Service attacks? Wouldn't it be trivial to pump traffic all the way through the DMZ to where EFT resides?

EFT is a file transfer server. It is meant to handle anything you can throw at it over the various listeners. EFT includes a number of DoS and flood-prevention mechanisms to mitigate these sorts of attacks. This would be the same if you stood up EFT (or any other FTP server) in the DMZ and terminated connections there. If EFT Server designates one or more IP addresses as needing to be blocked, it will add those IP addresses to its own internal IP Access Rules list and communicate that list to DMZ Gateway. DMZ Gateway will subsequently block all external clients with blacklisted IP addresses on the access list.

If there is a change to EFT's IP access rules, are the changes communicated immediately to the DMZ Gateway when those changes are applied?

Yes, IP address access policy changes (whether manually initiated or as a byproduct of an auto-ban) are automatically propagated to the DMZ Gateway (v3.0 and later). (Refer to Remote administrationfor information about banning IP addresses with a secure PNC.)

DMZ Gateway Knowledgebase Articles

For further assistance, refer to the following articles in the Globalscape Knowledgebase.

- #10023 - Changing the ping interval
- #10213 - When connecting to EFT Server via DMZ Gateway Server, how does authentication take place?
- #10367 - If DMZ Gateway Server hands all traffic to EFT Server on the inside network, wouldn't this be seen as a risk and defeat the objective of having the DMZ Gateway broker connections?
- #10686 - Connecting to a Remote Host Using DMZ Gateway as a Proxy
- #10710 - Overriding the default Profile limit in DMZ Gateway
- #10865 - Overriding the default Network Access Policy Exception limit in DMZ Gateway
- #10866 - Overriding the default SOCKS5 Connection Security in DMZ Gateway
- #11060 - Why isn't the Peer Notification Channel (PNC) encrypted?
- #11114 - Installing or Upgrading DMZ Gateway in a Failover (ACTIVE/PASSIVE) Cluster
- #11131 - Failed FTP connection after upgrading DMZ Gateway
- #11199 - Does the GHOST vulnerability affect any Globalscape products?
- #11201 - DMZ Gateway® Configuration Settings
- #11205 - Using CuteFTP® with DMZ Gateway® for testing remote EFT™ Connections
- #11206 - Running DMZ Gateway as non-root user in Linux
- #11270 - DMZ Gateway® Flood Protection Setting
- #11302 - Why do clients connect to EFT showing the IP of the Netscaler load balancer?
- #11390 - In the IP Access List in EFT, any "banned" IP addresses beyond the first 1000 are not blocked when DMZ Gateway is used.
- #11416 - EFT Site cannot connect to the second DMZ Gateway even though the host name matches
- #11434 - Specify to do DNS lookups on the EFT Server or DMZ Gateway Server
- #11447 - Can I use EFT and DMZ Gateway on separate networks, remote from each other, across a WAN?
- #11544 - Updating the Oracle JRE for DMZ Gateway

Check out https://kb.globalscape.com/KnowledgebaseCategory35.aspxoften as articles may have been added/removed since this was published.

Installing DMZ Gateway

The topics in this section provide instructions for installing DMZ Gateway.

- Installing DMZ Gateway on Windows Systems
- Installing DMZ Gateway on non-Windows Systems
- Installing DMZ Gateway in a Cluster
- Activating DMZ Gateway
- Manually Registering and Deregistering the DMZ Gateway Server Daemon
- Upgrading or Repairing DMZ Gateway
- Upgrading DMZ Gateway in a Cluster
- Uninstalling DMZ Gateway

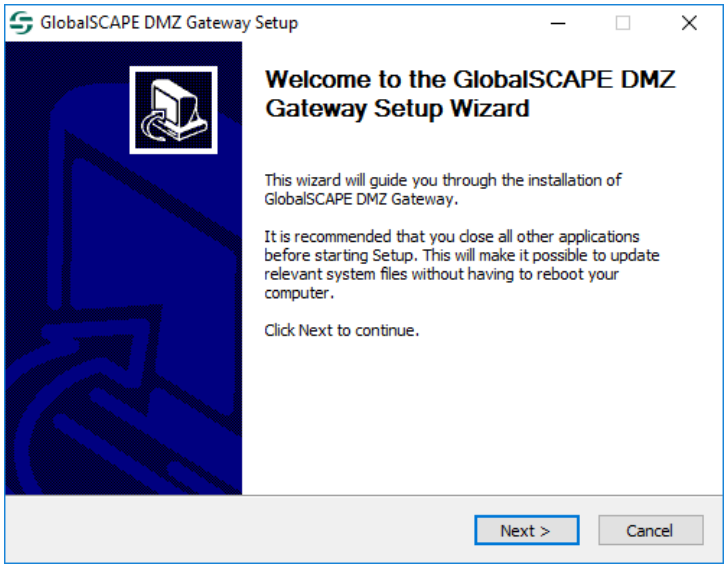
Installing DMZ Gateway on a Windows System

DMZ Gateway and the connecting application must be installed on separate computers.

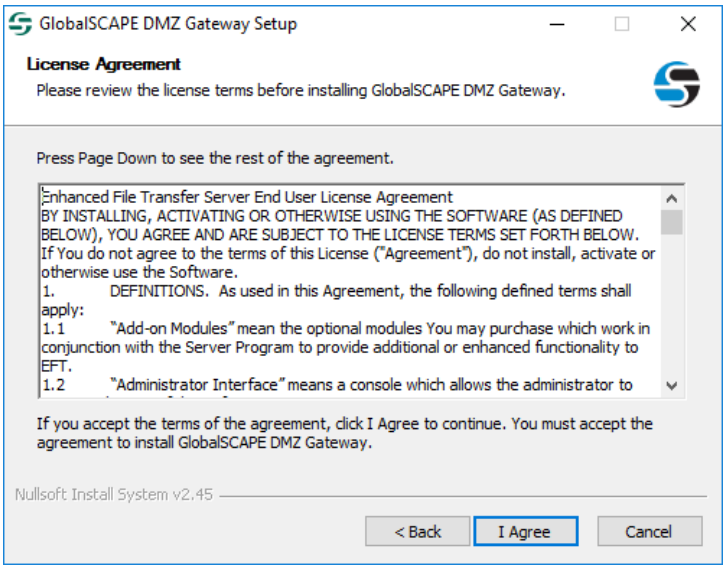
- If you are installing or upgrading DMZ Gateway in a cluster configuration, refer to Installing DMZ Gateway in a Cluster.
- If you are upgrading, refer to Upgrading or Repairing DMZ Gateway.

To install DMZ Gateway

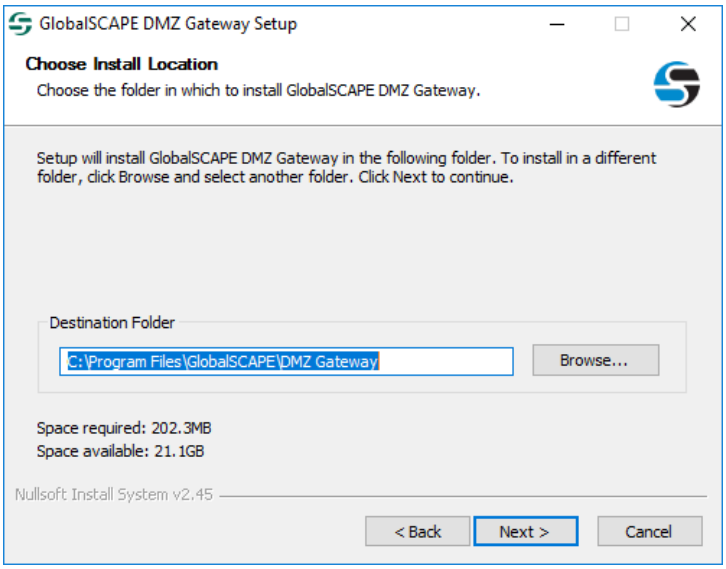
1. Close all unnecessary applications so that the installer can update system files without rebooting the computer.
2. Start the installer. The **Welcome** page appears.



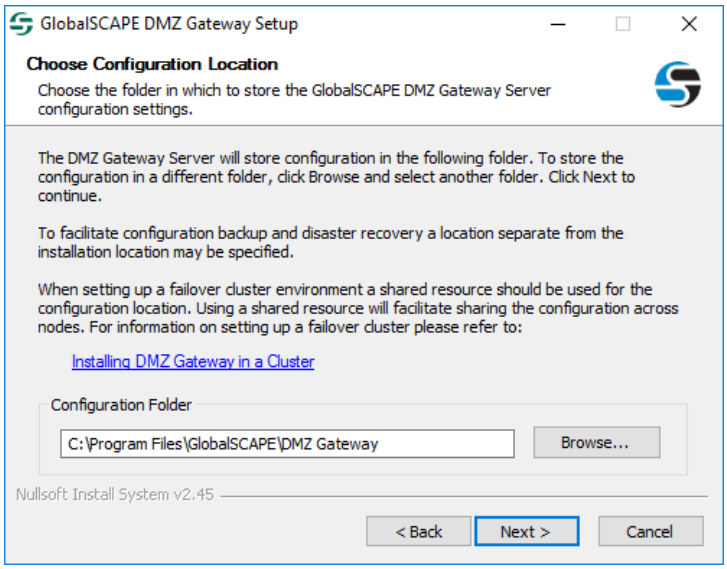
3. Click **Next**. The **License Agreement** appears.



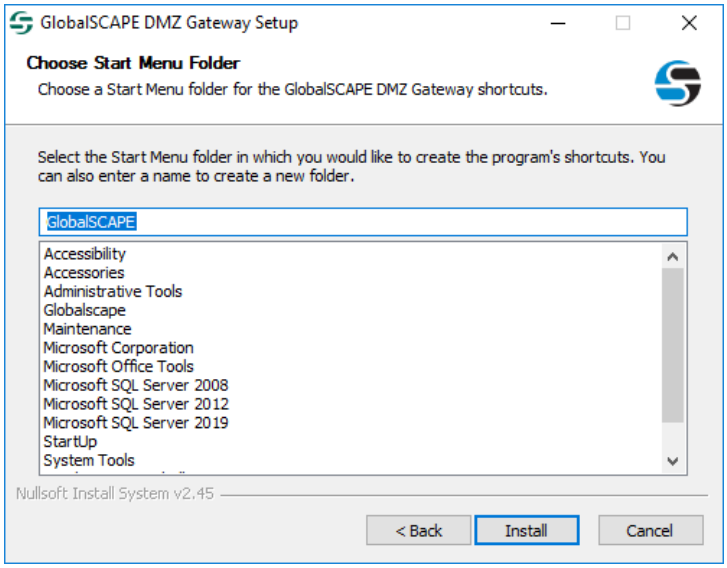
4. Read the license, then click **I Agree**.
5. If an existing installation is detected, refer to Upgrading or Repairing DMZ Gateway. Otherwise, the **Choose Installation Location** page appears.



6. The **Destination Folder** box displays the default location. Keep the default displayed in the box or click **Browse**to specify a different location. Also displayed is the amount of hard drive space required to install the program.
7. Click **Next**. The **Choose Configuration Location**page appears.

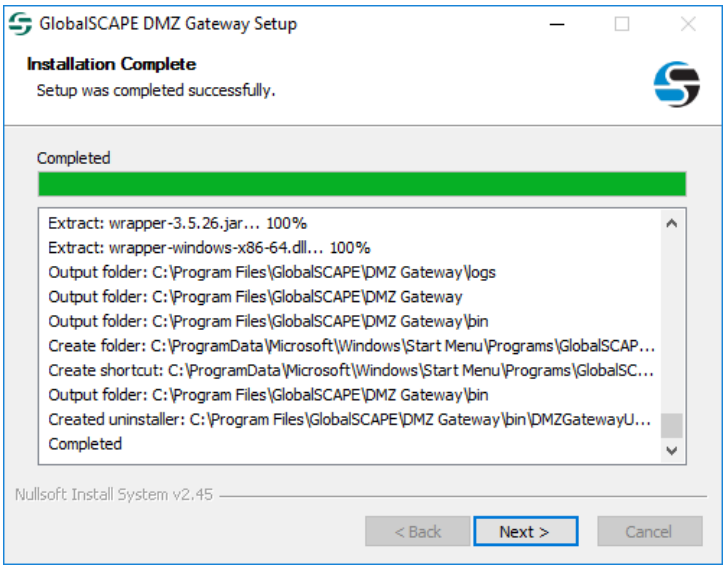


8. In the **Configuration Folder** box, specify the path at which to store configuration files for DMZ Gateway. The installation location is specified by default, but you can specify a separate location for backup and disaster recovery or for shared resources, such as with a cluster environment.
9. Click **Next**. The shortcuts page appears.

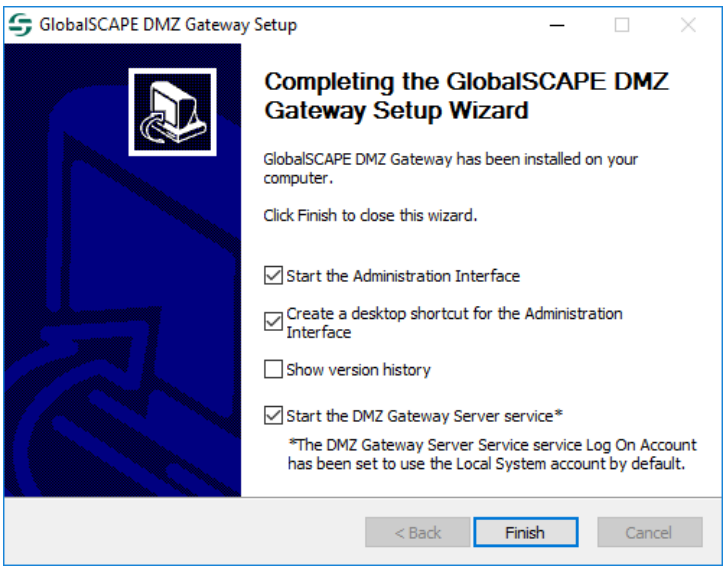


A shortcut to open the DMZ Gateway interface will be installed on the **Start** menu in a folder called **Globalscape**. You can keep this default location or specify a different location in which to install the shortcut.

10. Click **Install**. The product is installed and the installation log appears.



11. Click **Next**. The completed page appears.



The **Start the administration Interface**, **Create a desktop shortcut**, and **Start the DMZ Gateway Server service** check boxes are selected by default. Select the **Show version history**check box if you want to read the release notes. (You can also access the release notes in the installation folder.)

12. Click **Finish**. If you left the **Start the administration Interface** check box selected, the DMZ Gateway administration Interface appears.

A default Profile is defined that will listen on all IP addresses of the computer on which you installed DMZ Gateway. By default, it will listen for connections from servers on port 44500.

- Refer to Editing a Profile to change the IP address/port assignments.
- Refer to Creating a Profile to create new/additional Profiles.
- Refer to Controlling Access by IP Address to specify which IP addresses or IP masks are allowed or denied connections.

Activating DMZ Gateway

DMZ Gateway licensing is activated in the connecting application, not DMZ Gateway, which accepts connections from any licensed application. For example, a Single-Site license enables one EFT Site to connect to any available DMZ Gateway. A Multi-Site license enables one or more Sites from EFT to connect to any available DMZ Gateway. DMZ Gateway allows up to 15 Profile definitions to manage connections, but the license installed on the connecting application determines how many connections are allowed to DMZ Gateway.

After the trial has expired, you must activate DMZ Gateway by activating the serial number in the connecting application's administration interface. Refer to the EFT documentation for details of activating DMZ Gateway.

Licensing DMZ Gateway for EFT with the Accelerate Module

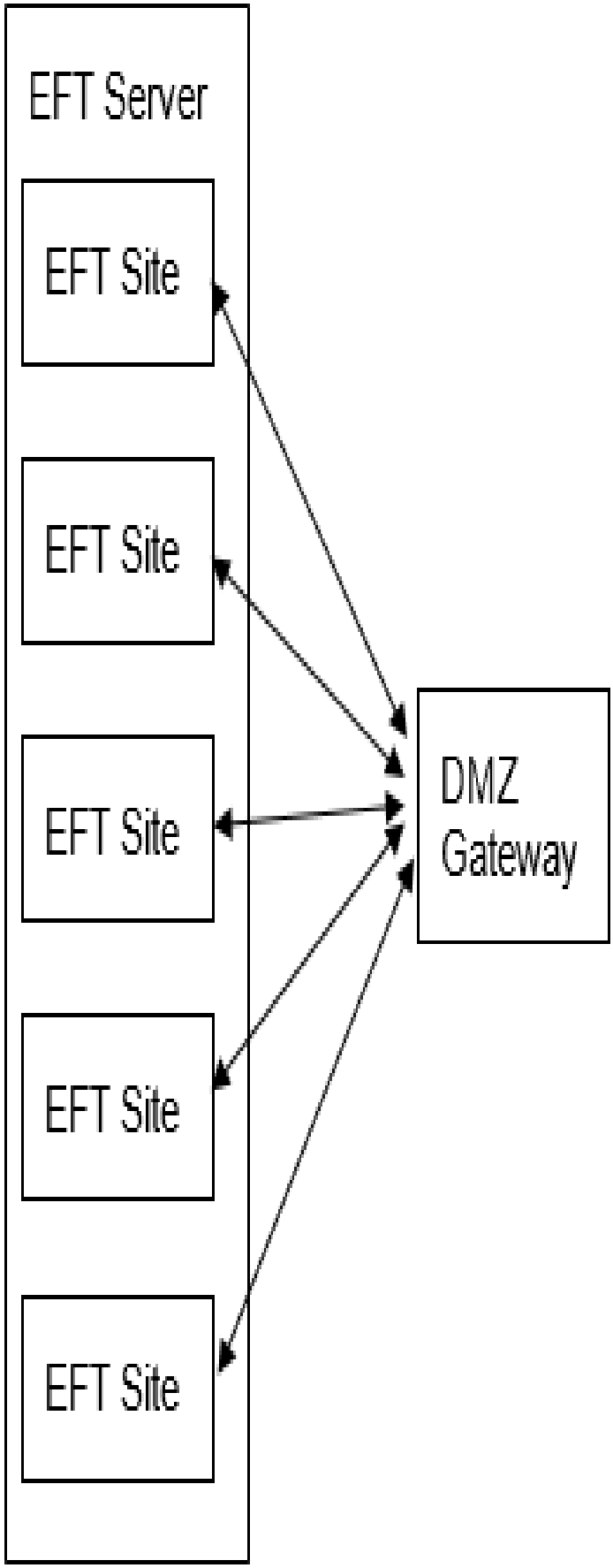
When licensing DMZ Gateway for EFT with the Accelerate module (available prior to EFT v8.0.5.7 for Windows only), not only do you have to activate DMZ Gateway (and the Accelerate module) in EFT, you also must install a license file in the DMZ Gateway installation directory, as described below, for each DMZ Gateway used.

To activate DMZ Gateways for EFT with the Accelerate module

1. Provide your DMZ Gateway server host's public-facing / forward-facing Internet Protocol (IP) address to your Globalscape point of contact. In return, you will receive two files derived from the supplied IP address:
    - DeiLicense.dat
    - FastImpl.dll
2. On the DMZ Gateway computer, stop the DMZ Gateway server service.
3. In the **\lib** folder of the DMZ Gateway installation folder (for example, **C:\Program Files\GlobalSCAPE\DMZ Gateway\lib**), replace the file FastImpl.dll with a new version provided by Globalscape.
4. In the **\conf** folder of the DMZ Gateway installation folder (for example, **C:\Program Files\GlobalSCAPE\DMZ Gateway\conf**), paste your license file (for example, DeiLicense.dat).
5. Start the DMZ Gateway server service.
    - DMZ Gateway will log the attempted registration and record its success or failure.
    - Registration is maintained upon upgrade or repair.
    - If the DMZ Gateway's host IP changes, you will need to request a new FastImpl.dll from Globalscape.

Activation Interaction between DMZ Gateway and EFT Trial

- When both EFT and DMZ Gateway are in trial mode, all DMZ Gateway features are enabled.
- If the EFT trial period expires (has not been activated) and the DMZ Gateway module has not been activated, EFT will:
  - Halt all outbound Peer Notification Channel (PNC) communication to the DMZ Gateway.
  - Disable all controls on EFT's DMZ Gateway configuration pages.
  - Disable the **Use EFT Server's DMZ Gateway as the proxy** check box in the Event Rule **Copy/Move** or **Download Action** wizards' **Proxy Settings** dialog box, which will cause any Event Rule to fail that uses DMZ Gateway as an outbound proxy.
  - Hide the **Perimeter Network Security** page of the Site Setup wizard in EFT.
  - Write a warning to the Windows Event Log: “EFT Server’s DMZ Gateway module evaluation period has expired.”
- If EFT is activated, but DMZ Gateway is in trial mode, the DMZ Gateway is fully functional until the DMZ Gateway trial expires. Once DMZ Gateway expires, all functionality and controls in EFT are disabled (unless you activate DMZ Gateway).
- If DMZ Gateway is activated using a single-Site serial number:
  - EFT allows only one EFT Site to connect to DMZ Gateway.
    - If during the trial period there were multiple Sites assigned to DMZ Gateways, all but one of the Site’s will disable their Gateway connection and write an error to the Windows Event Log
    - EFT will return an error if you attempt to connect another Site to a DMZ Gateway when one is already enabled and connected.
- If DMZ Gateway is activated using a multiple-Site serial number, EFT allows up to 15 EFT Sites on an EFT server to specify a DMZ Gateway to connect to.
  - A mulit-Site serial number cannot be used to connect multiple EFT servers to one or more DMZ Gateway servers:
    - There is a one-to-one correspondence of EFT servers to DMZ Gateway servers, even with a multi-Site DMZ Gateway serial number.
    - There can be a many-to-one correspondence of EFT Sites (an EFT construct) to a DMZ Gateway, with a multi-Site DMZ Gateway serial number


EFT Server
EFT Site
EFT Site
EFT Site
EFT Site
EFT Site
DMZ
Gateway

Installing DMZ Gateway on a non-Windows System

The installation process on each non-Windows operating system is the same, with a few minor differences. The basic process of installation can be described as follows:

1. Copy the appropriate installer archive file (**.tgz**) to the target machine.
2. Extract the contents of the installer archive. The archive contains two files: an installation script and an archive of the actual program files.
3. Run the installation script as root and follow the prompts.

The process for supported non-Windows operating systems is described below. (For installation on Windows systems, refer to Installing DMZ Gateway.)

The installation script includes registering and starting the DMZ Gateway server daemon (configuring it to auto-start on system start and auto-stop on system stop). Alternately, you can start the server manually using the command `<InstallDir>/bin/dmzgatewayd start`. Refer to Manually Registering and Deregistering the DMZ Gateway Server Daemon if you decide not to register the daemon during the installation process.

Installing DMZ Gateway on RedHat or SuSE Linux 32-Bit or 64-Bit

To install DMZ Gateway

1. Transfer the appropriate DMZ Gateway Linux installer archive to a convenient directory on the target machine.
2. On the target machine, open a terminal window. The installation package must be run with root privileges. If not already logged on as the root user, change to root using the `su`command in the terminal window.
3. Change to the directory containing the installer archive and perform the following:
   - On 32-bit systems:

     ```
     gunzip dmz-gateway-linux-x86-32.tgz
     tar xvf dmz-gateway-linux-x86-32.tar
     ./Install.sh
     ```

   - On 64-bit systems:

     ```
     gunzip dmz-gateway-linux-x86-64.tgz
     tar xvf dmz-gateway-linux-x86-64.tar
     ./Install.sh
     ```

4. Follow the prompts to complete the installation.
   - You are prompted to accept the license agreement, and to specify the installation and configuration directories (for example, **/opt/dmzgateway**), etc.
   - After everything is installed, you are prompted to register and start the DMZ Gateway daemon service.
   - If you start the service, you can execute the DMZ Gateway administration interface script (for example, type: `/opt/dmzgateway/bin/DMZGatewayadministrator`).

Installing DMZ Gateway on Ubuntu Linux 32-Bit or 64-Bit

To install DMZ Gateway

1. Transfer the DMZ Gateway installer archive into a convenient directory on the target machine.
2. On the target machine, open a terminal window.
3. Change to the directory containing the installer archive and perform the following:

- On 32-bit systems:

```
gunzip dmz-gateway-linux-x86-32.tgz
tar xvf dmz-gateway-linux-x86-32.tar
sudo ./Install.sh
```

- On 64-bit systems:

```
gunzip dmz-gateway-linux-x86-64.tgz
tar xvf dmz-gateway-linux-x86-64.tar
sudo ./Install.sh
```

4. Follow the prompts to complete the installation.
   - You are prompted to accept the license agreement, and to specify the installation and configuration directories (by default, **/opt/dmzgateway**), etc.
   - After everything is installed, you are prompted to register and start the DMZ Gateway daemon service.
   - If you start the service, you can execute the DMZ Gateway administration interface script (for example, type: `/opt/dmzgateway/bin/DMZGatewayadministrator`).

Solaris x86 32-Bit or 64-Bit

To install DMZ Gateway

1. Transfer the appropriate DMZ Gateway installer archive to a convenient directory on the target machine.
2. On the target machine, open a terminal window. The installation package must be run with root privileges. If not already logged on as the root user, change to root using the `su`command in the terminal window:
3. Change to the directory containing the installer archive and perform the following:
   - On 32-bit systems:

```
gunzip dmz-gateway-solaris-x86-32.tgz
tar xvf dmz-gateway-solaris-x86-32.tar
./Install.sh
```

   - On 64-bit systems:

```
gunzip dmz-gateway-solaris-x86-64.tgz
tar xvf dmz-gateway-solaris-x86-64.tar
./Install.sh
```

4. Follow the prompts to complete the installation.
    - You are prompted to accept the license agreement, and to specify the installation and configuration directories (for example, **/opt/dmzgateway**), etc.
    - After everything is installed, you are prompted to register and start the DMZ Gateway daemon service.
    - If you start the service, you can execute the DMZ Gateway administration interface script (for example, type: `/opt/dmzgateway/bin/DMZGatewayadministrator`).

Example of Installation Process on Solaris

Below is an example of executing the Install.sh script on a Solaris x86 32-bit computer.

```
== License Agreement ==
OMITTED - End-user License Agreement
Do you agree to the above license terms? [yes or no]:
 yes [ENTER]
== Choose Install Location ==
Please specify the path into which the DMZ Gateway program
 files will be installed or press "Enter" to accept the default.
Specify installation directory [/opt/dmzgateway]: [ENTER]
== Choose Configuration Location ==
Please specify the path in which to store the DMZ Gateway
 Server configuration settings or press "Enter" to accept the
 default.
Specify configuration directory [/opt/dmzgateway]:
/export/home/appdata
 [ENTER]
== Choose Installation Owner ==
Please specify the user account name to use as the owner
 of the installed files.
Specify owner [root]: [ENTER]
== Choose Installation Group ==
Please specify the user group name to use as the group
 of the installed files.
Specify group [root]: [ENTER]
== Confirm Settings ==
Installation directory:  /opt/dmzgateway Configuration
 directory: /export/home/appdata Installation owner:      root
 Installation group:      root
Are these settings correct? [yes or no]: yes [ENTER]
Creating directory "/opt/dmzgateway"
Creating directory "/export/home/appdata"
Unpacking archive...
```

```
Extracting files...
OMITTED - Extracted Program File List
Unpacking JRE...
Extracting JRE...
OMITTED - Extracted Java Runtime Environment File List
Removing temporary files...
Updating permissions...
Updating ownership...
Updating configuration file...
== Register Service ==
The installation script can attempt to register the DMZ
 Gateway Server daemon service (dmzgatewayd) for automatic
startup and
 shutdown.
Register the DMZ Gateway Server daemon service? [yes
 or no]: yes
Creating symbolic link "/etc/init.d/dmzgatewayd"...
Registering system daemon...
ln -sf /etc/init.d/dmzgatewayd /etc/rc0.d/K99dmzgatewayd
ln -sf /etc/init.d/dmzgatewayd /etc/rc1.d/K99dmzgatewayd
ln -sf /etc/init.d/dmzgatewayd /etc/rc2.d/S99dmzgatewayd
ln -sf /etc/init.d/dmzgatewayd /etc/rc3.d/S99dmzgatewayd
== Start Service ==
The installation script can attempt to start the DMZ
 Gateway Server daemon service (dmzgatewayd).
Start the DMZ Gateway Server daemon service? [yes or
 no]:  yes [ENTER]
Executing: /etc/init.d/dmzgatewayd start
-n Starting DMZ Gateway Server...
== Installation Complete ==
The DMZ Gateway is now installed.
The DMZ Gateway Server daemon service may be controlled
 using the "dmzgatewayd" script:
/opt/dmzgateway/bin/dmzgatewayd
The DMZ Gateway administration Interface may be started
 using the script:
/opt/dmzgateway/bin/DMZGatewayAdmin
```

Manually Registering and Deregistering the DMZ Gateway Daemon (non-Windows Systems)

During the installation process, you are prompted to register the DMZ Gateway server daemon (configuring it to auto-start on system start and auto-stop on system stop). If you choose not to register the daemon during the installation process, use the procedure below to add or remove the DMZ Gateway daemon script, dmzgatewayd, from automatic system startup and shutdown.

There are multiple methods of configuring a daemon script for automatic startup/shutdown on Linux/Solaris. Ultimately, whatever method is used typically results in the creation of symbolic links in the **/etc/rc***directories. These scripts are called at different startup and shutdown run levels of the operating system to start and stop the daemon.

RedHat Enterprise Linux

After creation of the **/etc/init.d/dmzgatewayd**symbolic link, the **chkconfig** command can be used to register and deregister the script for system startup/shutdown.

To register the script

- The following command may be used as root:

  ```
  chkconfig
          --add dmzgatewayd
  ```

  (there are two dashes before `add`)

To deregister the script

- The following command may be used as root:

  ```
  chkconfig
          --del dmzgatewayd
  ```

  (there are two dashes before `del`)

SuSE Linux

After creation of the **/etc/init.d/dmzgatewayd**symbolic link, the **insserv**command can be used to register and deregister the script for system startup/shutdown.

To register the script

- The following command may be used as root:

```
insserv
        dmzgatewayd
```

To deregister the script

- The following command may be used as root:

```
insserv
        -r dmzgatewayd
```

Ubuntu Linux

After creation of the **/etc/init.d/dmzgatewayd**symbolic link, the **update-rc.d**command can be used to register and deregister the script for system startup/shutdown.

To register the script

- The following command may be used as root:

```
update-rc.d
        dmzgatewayd defaults
```

To deregister the script

- The **/etc/init.d/dmzgatewayd**symbol link must first be removed using the following command as root:

```
rm /etc/init.d/dmzgatewayd
```

To deregister the daemon

- The following command may be used as root:

```
update-rc.d
        dmzgatewayd remove
```

Solaris

On Solaris, after creation of the **/etc/init.d/dmzgatewayd**symbolic link you typically manually create the appropriate symbolic links in the **/etc/rc*** directories.

To register the script

- The following commands may be used as root:

```
ln -sf
        /etc/init.d/dmzgatewayd /etc/rc0.d/K99dmzgatewayd

ln -sf /etc/init.d/dmzgatewayd /etc/rc1.d/K99dmzgatewayd

ln -sf /etc/init.d/dmzgatewayd /etc/rc2.d/S99dmzgatewayd

ln -sf /etc/init.d/dmzgatewayd /etc/rc3.d/S99dmzgatewayd
```

To deregister the script

- Remove the symbolic links as root:

```
rm /etc/rc0.d/K99dmzgatewayd

rm /etc/rc1.d/K99dmzgatewayd

rm /etc/rc2.d/S99dmzgatewayd

rm /etc/rc3.d/S99dmzgatewayd
```

Uninstalling DMZ Gateway

Use the applicable procedure below to uninstall DMZ Gateway.

Uninstalling DMZ Gateway on a Windows System

Uninstall DMZ Gateway using Windows' **Add/Remove Programs** tool or via the shortcut on the **Start** menu.

Uninstalling DMZ Gateway on a non-Windows System

The installation process on each non-Windows operating system is the same with a few minor differences. The basic process of installation can be described as follows:

- Run the uninstallation script as root and follow the prompts. (The script is created during installation and is `<InstallDir>/bin/Uninstall.sh`)

RedHat Enterprise Linux, SuSE Linux, or Solaris x86 32-Bit or 64-Bit

You can uninstall DMZ Gateway using the Uninstall.sh script located in the `<InstallDir>/bin`directory.

To uninstall DMZ Gateway

1. On the target machine, open a terminal window. The uninstall script must be run with root privileges. If not already logged on as the root user, change to root using the su command in the terminal window:

   ```
   su
   ```

2. Run the Uninstall.sh script:

   ```
   /<InstallDir>/bin/Uninstall.sh
   ```

   For example:

   ```
   /opt/dmzgateway/bin/Uninstall.sh
   ```

3. Follow the prompts to complete uninstalling.

Ubuntu Linux 32-Bit or 64-Bit

You can uninstall DMZ Gateway using the Uninstall.sh script located in the <InstallDir>/bin directory.

To uninstall DMZ Gateway on Ubuntu Linux

1. On the target machine, open a terminal window.
2. Run the Uninstall.sh script:

   ```
   sudo /<InstallDir>/bin/Uninstall.sh
   ```

   For example:

   ```
   sudo /opt/dmzgateway/bin/Uninstall.sh
   ```
3. Follow the prompts to complete uninstalling.

Example of Uninstallation Process on Solaris

The following printout is a sample execution of the **Uninstall.sh**installation script run on Solaris x86 32-bit.

```
== Confirm Uninstallation == The uninstallation script
 will now uninstall the DMZ Gateway from the following
installation directory:
/opt/dmzgateway
Proceed with uninstallation? [yes or no]: yes [ENTER]


== Stop Service == The installation script has detected
 that the DMZ Gateway Server daemon service (dmzgatewayd) is
currently
 running. The service must be stopped before proceeding. The
script can
 now attempt to stop the service.
Stop the DMZ Gateway Server daemon service? [yes or no]:
 yes [ENTER]
Executing: /etc/init.d/dmzgatewayd stop Stopping DMZ Gateway
 Server... Stopped DMZ Gateway Server.


== Deregister Service == The installation script can attempt
 to deregister the DMZ Gateway Server daemon service
(dmzgatewayd) from
 automatic startup and shutdown.
Deregister the DMZ Gateway Server daemon service? [yes
 or no]: yes [ENTER]
Removing /etc/init.d/dmzgatewayd symbolic link...
Deregistering system daemon:
rm /etc/rc0.d/K99dmzgatewayd rm /etc/rc1.d/K99dmzgatewayd
 rm /etc/rc2.d/S99dmzgatewayd rm /etc/rc3.d/S99dmzgatewayd
Removing installation files...
== Uninstallation Complete ==
```

Upgrading or Repairing DMZ Gateway

You must upgrade DMZ Gateway before upgrading EFT.

To upgrade or repair DMZ Gateway on non-Windows systems

- Perform the standard installation process for the target operating system and use the same settings for installation path and configuration path. If the DMZ Gateway Server daemon service is running, you are prompted to stop it; if you do not stop it, the installer will abort.

To upgrade on Windows systems

1. Close the administration interface.
2. As a precaution, back up the existing installation directories and any other files you may have installed elsewhere.
3. Launch the installer and then click **Next**. The **License Agreement** appears.
4. Click **I Agree**. The installer will detect an existing installation.
5. The older version must be uninstalled. You can keep the existing configuration or use the (new) default configuration. Click one of the following, then click **Next:**
    - Keep existing configuration and uninstall the older version
    - Use a default configuration and uninstall the older version
6. Follow the prompts to finish the upgrade. Refer to Installing DMZ Gateway, if necessary.

    During the upgrade process, the DMZ Gateway service **Log On As** account is set to use the **Local System** account.

To upgrade from DMZ Gateway 3.x on Windows systems

1. Close the administration interface.
2. Launch the installer. The installer will detect an existing installation.
3. After accepting the End-User License Agreement, click **Upgrade DMZ Gateway**, then click **Upgrade**.
4. Follow the prompts to finish the upgrade. Refer to Installing DMZ Gateway, if necessary.

To reinstall DMZ Gateway 3.x on Windows systems

Reinstallation can be used to fix installations in situations where program files have been corrupted or accidentally deleted. During reinstallation, the installer will reinstall

the original copies of corrupted or missing program files.

1. Close the administration interface.
2. Launch the installer. The installer will detect an existing installation.
3. After accepting the End-User License Agreement, click **Reinstall DMZ Gateway**, then click **Reinstall**.
4. Follow the prompts to finish the reinstall. Refer to Installing DMZ Gateway, if necessary.

Interface Reference

The topics in this section describe the dialog boxes in DMZ Gateway that have **Help** buttons and provide a list of frequently used commands.

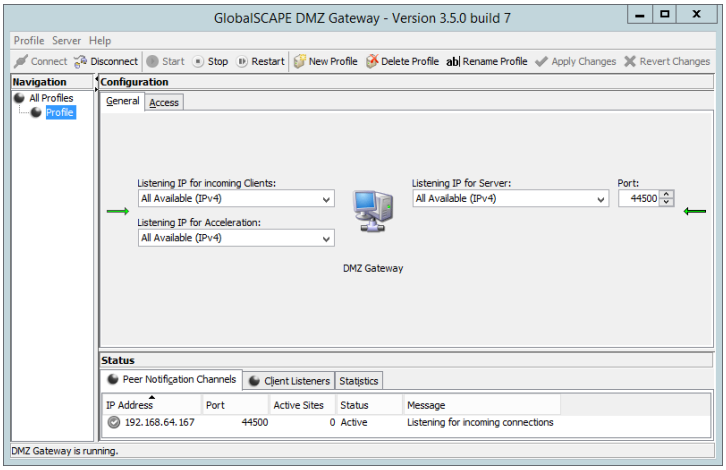
- The DMZ Gateway Interface
- IP Access Exception Dialog Box
- New Profile Wizard--Profile name
- New Profile Wizard--Peer Server Access
- New Profile Wizard--Configuration
- Frequently Used Commands

The DMZ Gateway Interface

The DMZ Gateway interface is used for mapping and viewing DMZ Gateway connections. *Profiles* are used to define connections to DMZ Gateway.

To open the interface

- On Windows systems, double-click the DMZ Gateway shortcut on the desktop or **Start** menu.
- On non-Windows systems, after the server service has started, execute the DMZ Gateway administration interface script (for example, `/opt/dmzgateway/bin/DMZGatewayadministrator`). On SuSe Linux, you must be logged in as root to launch the administration interface.
- The left pane displays each of the defined *Profiles*in an expandable/collapsible tree view. DMZ Gateway has a default Profile for which you define the listening IP address(es) and port for the connecting application, listening IP address(es) for connecting clients, and the IP address ban list. When DMZ Gateway connects, only the default Profile is displayed. The interface displays the configuration for the last Profile modified or viewed the last time the interface was opened or the first (default) Profile if no "last viewed" profile value is available.
- In the default view, with **All Profiles** selected, the right pane displays the status of the DMZ Gateway service and the status of all Profiles.
- When a Profile is selected, the right pane displays the configuration information and status of the selected Profile.



DMZ Gateway Administration Interface PID File

When the DMZGatewayadministrator executable is launched it will create the PID file <Installation Directory>\DMZGatewayadministrator.pid. This file contains the PID for the administration interface process. The timestamp of the file is updated every 10 seconds while the administration interface is running. When the application exits gracefully, it deletes the PID file.

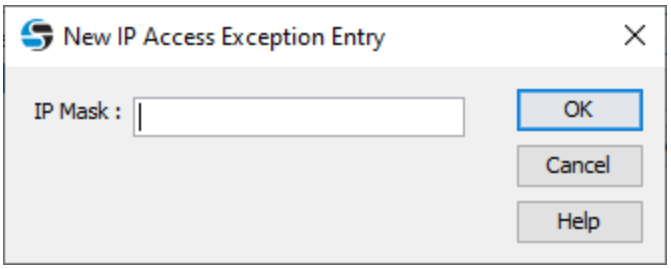
This file is also used to prevent simultaneous execution of multiple copies of the administration interface. When the administration interface starts, it checks for the presence of the PID file. If the file exists and its timestamp has been updated in the last 20 seconds it will assume another copy of the user interface is running and exit.

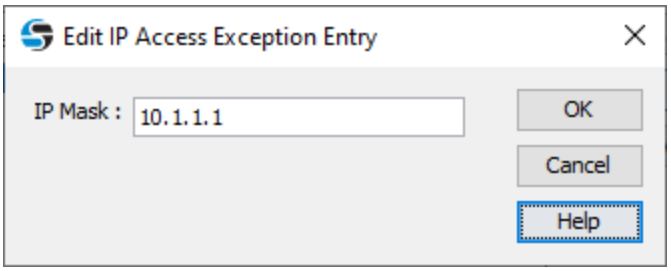
Related Topics

- Refer to Creating a Profile for information about Profile configuration.
- Refer to Controlling Access by IP Address for information about granting or denying access to a specific IP addresses or an IP mask.
- Refer to Starting and Stopping the DMZ Gateway Server Service for details of stopping and starting the DMZ Gateway server service.
- Refer to Viewing Statistics for details of each of the tabs in the **Status**pane.

IP Access Exception Entry Dialog Box

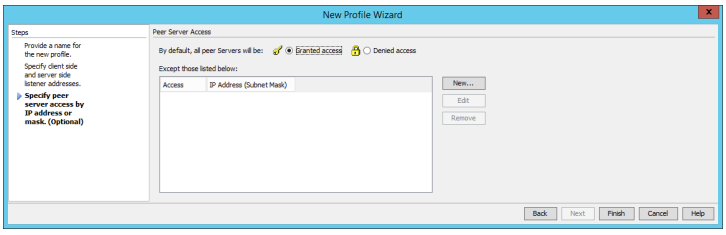
Use the **New IP Access Exception Entry** dialog box and the **Edit IP Access Exception Entry** dialog box to provide a specific IP address (for example, 192.168.43.201) or an IP address mask using wildcards (for example, 192.168.43.*).





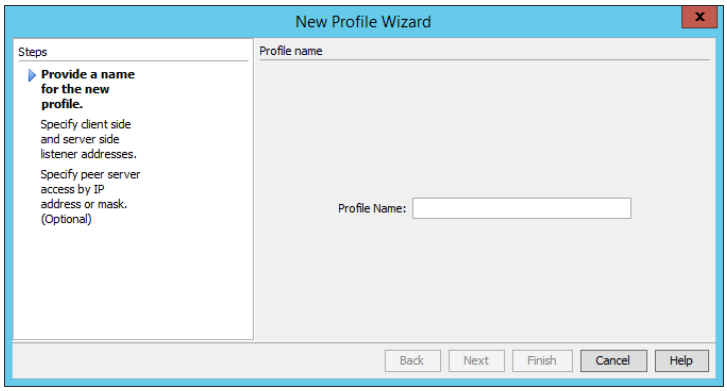
To specify the IP address or mask

1. In the **IP Mask** box, specify the IP address or range of IP addresses to which you are denying or granting access. You can use wildcards to select ranges of IP addresses.
2. Click **OK.** The IP address/mask appears in the exceptions list on the **Peer Server Access** tab.



New Profile Wizard--Profile name

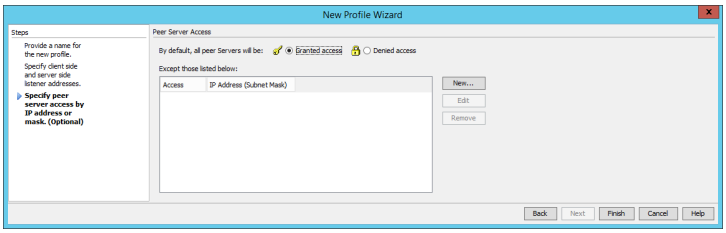
The New Profile Wizard is used to define a new Profile.



In the **Profile Name** box, provide a unique name for this Profile. The name will appear in the interface, logs, error messages, and reports.

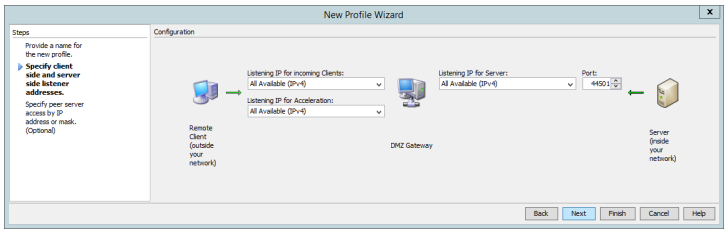
New Profile Wizard--Peer Server Access

Use the **Peer Server Access** page to specify the IP addresses or IP masks of peer servers who are allowed or denied access to DMZ Gateway. All IP addresses are granted access by default. Refer to IP Access Exception Dialog Box for details.



New Profile Wizard--Configuration

Use the **Configuration** page of the wizard to specify which IP address/port combination on the DMZ Gateway computer should be used as the listening IP addresses.



To specify the client side and server side listening addresses

1. In the **Listening IP** boxes, click the down arrow to select the IP address or leave the default of **All Available**. Refer to Specifying the Listening IP Addresses for detailed information.
2. In the **Port** box, specify the port on which DMZ Gateway communicates with the server. The default is **44500**. The connection will be refused if the IP address is on the IP address ban list.

Frequently Used Non-Windows Commands

The table below describes several commands that you use to administer DMZ Gateway on non-Windows platforms. The commands are described in the applicable procedures in more detail; this table is provided only as a quick reference.

In the examples below, *your file and path names may differ.*

Install

Platform: All

Example:

```
gunzip dmz-gateway-linux-x86-32.tgz

tar xvf dmz-gateway-linux-x86-32.tar

./Install.sh
```

Register the script

Platform: Redhat

Example:

```
chkconfig --add dmzgatewayd
```

Platform: Suse

Example:

```
insserv dmzgatewayd
```

Platform: Ubuntu

Example:

```
update-rc.d dmzgatewayd defaults
```

Platform: Solaris

Example:

```
ln -sf /etc/init.d/dmzgatewayd
 /etc/rc0.d/K99dmzgatewayd

ln -sf /etc/init.d/dmzgatewayd
 /etc/rc1.d/K99dmzgatewayd

ln -sf /etc/init.d/dmzgatewayd
 /etc/rc2.d/S99dmzgatewayd

ln -sf /etc/init.d/dmzgatewayd
 /etc/rc3.d/S99dmzgatewayd
```

Deregister the script

Platform: Redhat

Example:

```
chkconfig --del dmzgatewayd
```

Platform: Suse

Example:

```
insserv -r dmzgatewayd
```

Platform: Ubuntu

Example:

```
rm /etc/init.d/dmzgatewayd

update-rc.d dmzgatewayd remove
```

Platform: Solaris

Example:

```
rm /etc/rc0.d/K99dmzgatewayd

rm /etc/rc1.d/K99dmzgatewayd
```

```
rm /etc/rc2.d/S99dmzgatewayd

rm /etc/rc3.d/S99dmzgatewayd
```

Uninstall

Platform: All

Example:

```
/opt/dmzgateway/bin/Uninstall.sh
```

Open the DMZ Gateway Interface

Platform: All

Example:

```
/opt/dmzgateway/bin/DMZGatewayadministrator
```

Start DMZ Gateway Server service

Platform: All

Example:

```
/opt/dmzgateway/bin/dmzgatewayd start
```

Stop DMZ Gateway Server service

Platform: All

Example:

```
/opt/dmzgateway/bin/dmzgatewayd
 stop
```

Administering DMZ Gateway

The topics in this section provide instructions for administering DMZ Gateway.

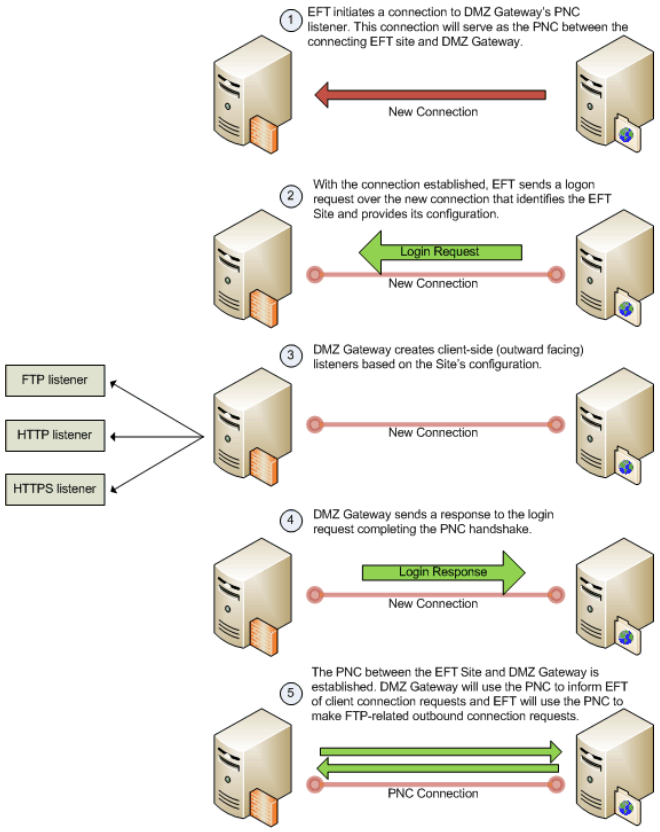
- Initialization and Connection Diagrams
- Frequently Used Commands
- Allow LDAP Authentication through DMZ Gateway
- Controlling Access by IP Address
- Default Network Ports for EFT and DMZ Gateway
- Creating a DMZ Gateway Profile
- Editing a Profile
- Deleting a Profile
- Renaming a Profile
- DMZ Gateway Components
- DMZ Gateway System Files
- DMZ Gateway Headless Administration
- DMZ Gateway Logging
- DMZ Gateway Server Configuration File (gwconfig.xml) Reference
- DMZ Gateway Server Unix/Solaris Daemon
- DMZ Gateway Status
- Internal Domain Settings
- Routing AS2 Traffic through DMZ Gateway
- Specifying the Listening IP Address
- Starting and Stopping the DMZ Gateway Server Service
- Testing the Configuration
- Troubleshooting DMZ Gateway Communication
- Using DMZ Gateway as an Outbound Proxy
- Viewing Statistics

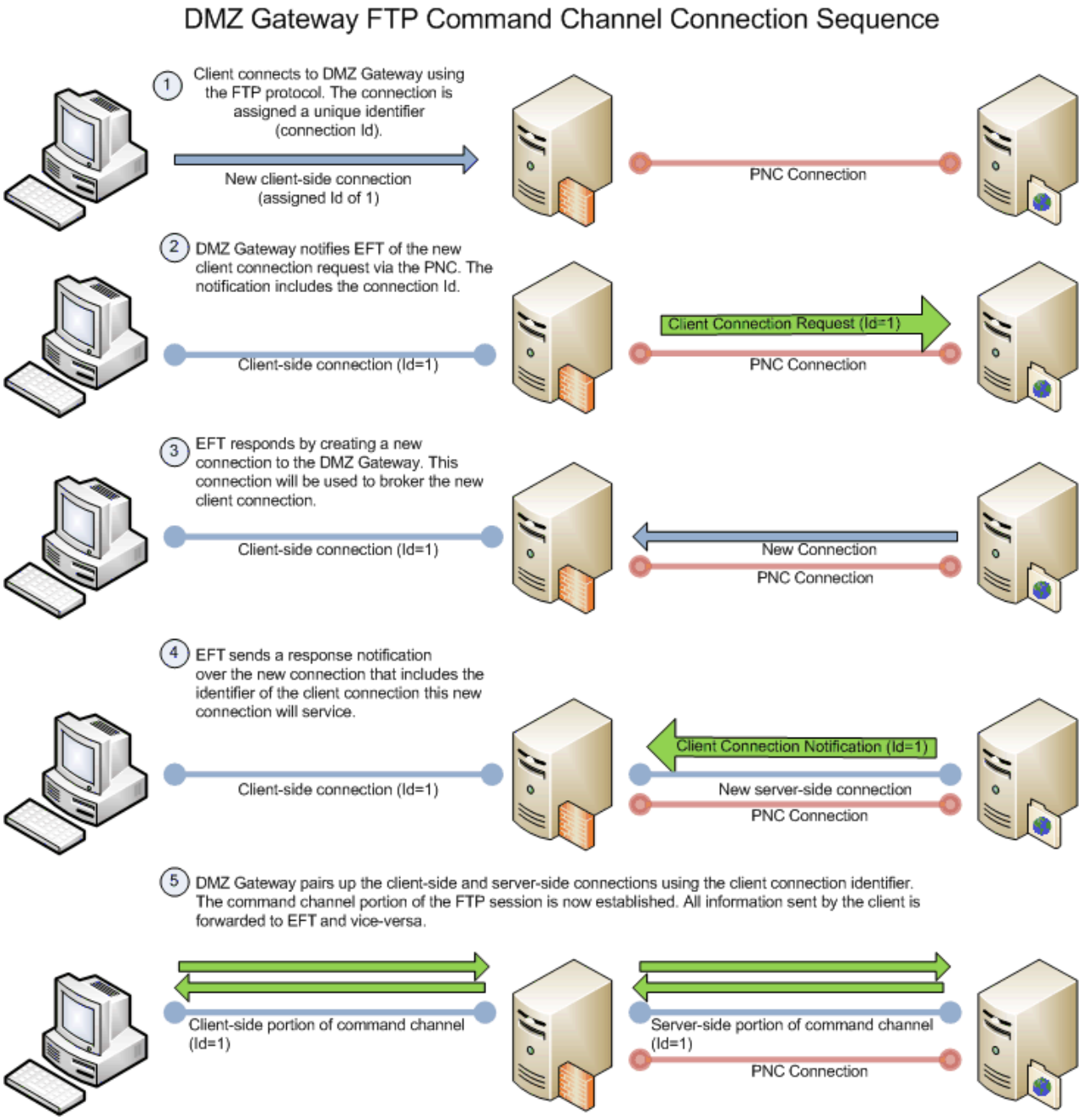
See also: Knowledgebase article: Specify Whether DNS Lookup is Performed on EFT or DMZ

Initialization and Connection Diagrams

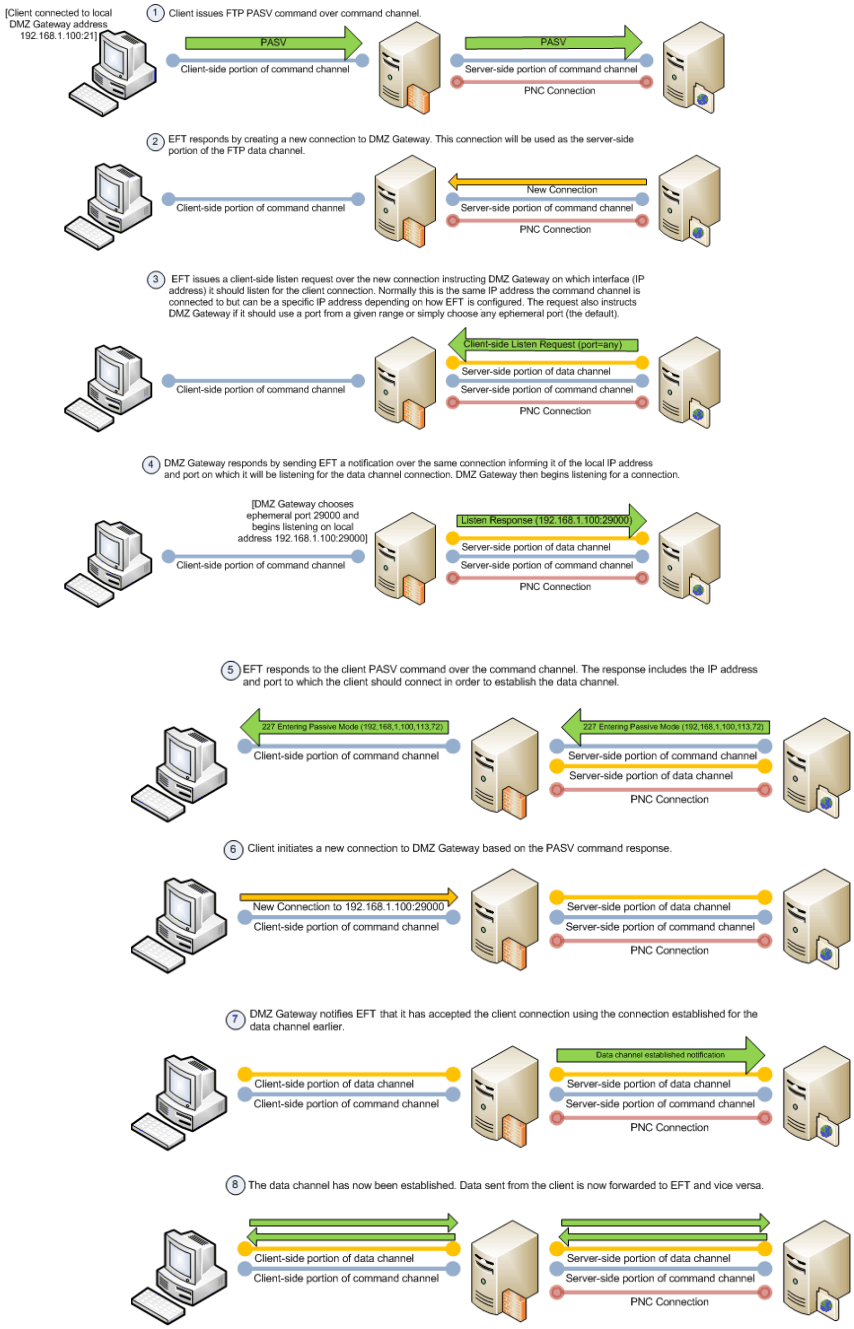
The diagrams below illustrate the initialization and connection sequences for DMZ Gateway and EFT communication.

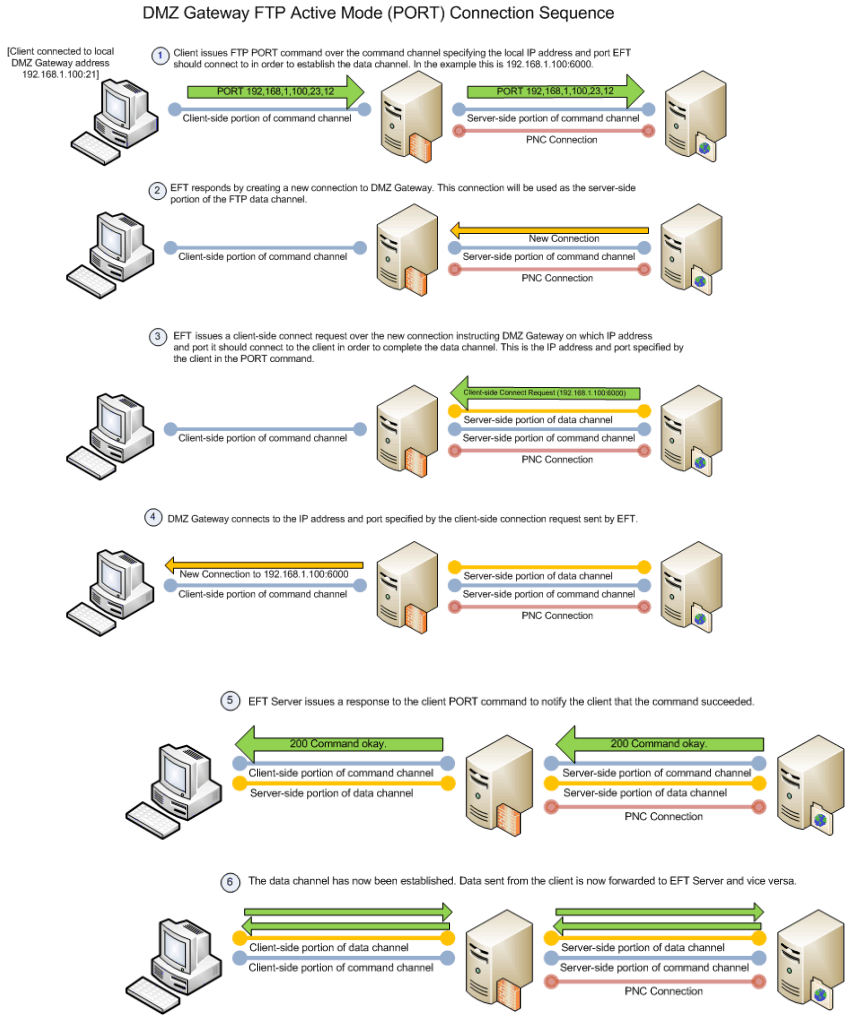
DMZ Gateway Peer Notification Channel (PNC) Initialization Sequence




DMZ Gateway FTP Command Channel Connection Sequence
1
Client connects to DMZ Gateway using the FTP protocol. The connection is assigned a unique identifier (connection Id).
New client-side connection (assigned Id of 1)
PNC Connection
2
DMZ Gateway notifies EFT of the new client connection request via the PNC. The notification includes the connection Id.
Client-side connection (Id=1)
Client Connection Request (Id=1)
PNC Connection
3
EFT responds by creating a new connection to the DMZ Gateway. This connection will be used to broker the new client connection.
Client-side connection (Id=1)
New Connection
PNC Connection
4
EFT sends a response notification over the new connection that includes the identifier of the client connection this new connection will service.
Client-side connection (Id=1)
Client Connection Notification (Id=1)
New server-side connection
PNC Connection
5
DMZ Gateway pairs up the client-side and server-side connections using the client connection identifier. The command channel portion of the FTP session is now established. All information sent by the client is forwarded to EFT and vice-versa.
Client-side portion of command channel (Id=1)
Server-side portion of command channel (Id=1)
PNC Connection

DMZ Gateway FTP Passive Mode (PASV) Connection Sequence




DMZ Gateway FTP Active Mode (PORT) Connection Sequence
[Client connected to local DMZ Gateway address 192.168.1.100:21]
1 Client issues FTP PORT command over the command channel specifying the local IP address and port EFT should connect to in order to establish the data channel. In the example this is 192.168.1.100:6000.
PORT 192,168,1,100,23,12
Client-side portion of command channel
PORT 192,168,1,100,23,12
Server-side portion of command channel
PNC Connection
2 EFT responds by creating a new connection to DMZ Gateway. This connection will be used as the server-side portion of the FTP data channel.
Client-side portion of command channel
New Connection
Server-side portion of command channel
PNC Connection
3 EFT issues a client-side connect request over the new connection instructing DMZ Gateway on which IP address and port it should connect to the client in order to complete the data channel. This is the IP address and port specified by the client in the PORT command.
Client-side portion of command channel
Client-side Connect Request (192.168.1.100:6000)
Server-side portion of data channel
Server-side portion of command channel
PNC Connection
4 DMZ Gateway connects to the IP address and port specified by the client-side connection request sent by EFT.
New Connection to 192.168.1.100:6000
Client-side portion of command channel
Server-side portion of data channel
Server-side portion of command channel
PNC Connection
5 EFT Server issues a response to the client PORT command to notify the client that the command succeeded.
200 Command okay.
Client-side portion of command channel
Server-side portion of data channel
200 Command okay.
Server-side portion of command channel
Server-side portion of data channel
PNC Connection
6 The data channel has now been established. Data sent from the client is now forwarded to EFT Server and vice versa.
Client-side portion of data channel
Client-side portion of command channel
Server-side portion of data channel
Server-side portion of command channel
PNC Connection

Frequently Used Non-Windows Commands

The table below describes several commands that you use to administer DMZ Gateway on non-Windows platforms. The commands are described in the applicable procedures in more detail; this table is provided only as a quick reference.

In the examples below, *your file and path names may differ.*

Install

Platform: All

Example:

```
gunzip dmz-gateway-linux-x86-32.tgz

tar xvf dmz-gateway-linux-x86-32.tar

./Install.sh
```

Register the script

Platform: Redhat

Example:

```
chkconfig --add dmzgatewayd
```

Platform: Suse

Example:

```
insserv dmzgatewayd
```

Platform: Ubuntu

Example:

```
update-rc.d dmzgatewayd defaults
```

Platform: Solaris

Example:

```
ln -sf /etc/init.d/dmzgatewayd
 /etc/rc0.d/K99dmzgatewayd

ln -sf /etc/init.d/dmzgatewayd
 /etc/rc1.d/K99dmzgatewayd

ln -sf /etc/init.d/dmzgatewayd
 /etc/rc2.d/S99dmzgatewayd

ln -sf /etc/init.d/dmzgatewayd
 /etc/rc3.d/S99dmzgatewayd
```

Deregister the script

Platform: Redhat

Example:

```
chkconfig --del dmzgatewayd
```

Platform: Suse

Example:

```
insserv -r dmzgatewayd
```

Platform: Ubuntu

Example:

```
rm /etc/init.d/dmzgatewayd

update-rc.d dmzgatewayd remove
```

Platform: Solaris

Example:

```
rm /etc/rc0.d/K99dmzgatewayd

rm /etc/rc1.d/K99dmzgatewayd
```

```
rm /etc/rc2.d/S99dmzgatewayd

rm /etc/rc3.d/S99dmzgatewayd
```

Uninstall

Platform: All

Example:

```
/opt/dmzgateway/bin/Uninstall.sh
```

Open the DMZ Gateway Interface

Platform: All

Example:

```
/opt/dmzgateway/bin/DMZGatewayadministrator
```

Start DMZ Gateway Server service

Platform: All

Example:

```
/opt/dmzgateway/bin/dmzgatewayd start
```

Stop DMZ Gateway Server service

Platform: All

Example:

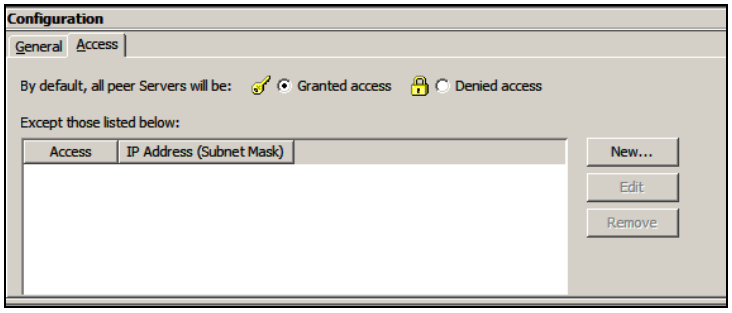
```
/opt/dmzgateway/bin/dmzgatewayd
 stop
```

Controlling Access by IP Address

By default, all IP addresses are granted access to DMZ Gateway. You can grant access to only one specific IP address or a range of IP addresses, or deny access to one specific address or a range of addresses. You can define up to 100 IP address masks.

To grant/deny access by IP Address

1. In the Profile tree, click the default **Profile**or create a new profile.
2. In the **Configuration** pane, click the **Access**tab. The exception list appears.



3. The **Access** tab displays the IP addresses that are granted or denied access. By default, all IP addresses are granted access, and no exceptions are displayed in the list.
4. To configure exceptions, click **Granted access**or **Denied access**.
   - If most IP addresses are *allowed* access, click **Granted access**, then add the exceptions (IP addresses that are not allowed access).
   - If most IP addresses are *denied* access, click **Denied access**, then add the exceptions (IP addresses that are allowed access).

   NOTE: For example, if you want to allow only 192.168.174.159 and block every other IP address, click **Denied access**, click **Add**, then type `192.168.174.159`in the **IP mask** box. This will deny access to all IP addresses except 192.168.174.159.

5. Click **Add**. The **New IP Access Exception Entry**dialog box appears.
6. Specify the IP address or range of IP addresses to which you are denying or granting access. You can use wildcards to select ranges of IP addresses.
7. Click **OK.**The IP address/mask appears in the exceptions list.
8. Click **Apply Changes** to save the changes on DMZ Gateway.

Default Network Ports for EFT and DMZ Gateway

The table below provides information about the default network ports used for clients (that is, browsers and web clients) and services such as AS2 and web services.

Ports	Purpose
EFT File Transfers protocols	
TCP: 443 (HTTPS)	**Inbound**: Encrypted web connections for transferring files with EFT used by clients (browsers, web clients) and the services such: AS2, Mobile Transfer Client Invoke event rules via Web Services EFT account management (password changed) **Outbound**: Encrypted web connections used by EFT to transfer files via HTTPS with other application servers.
TCP: 80 (HTTP)	**Inbound**: Unencrypted web connections to transferring files with EFT used by clients (browsers, web clients) and other application servers. **Outbound**: Unencrypted web connections used by EFT to transfer files via HTTP with other application servers.
TCP: 22 (SFTP)	**Inbound**: Encrypted TCP connections for transferring files with EFT via SFTP protocol used by SFTP clients. **Outbound**: Encrypted TCP connections used by EFT to transfer files via SFTP protocol with other SFTP servers.
TCP: 21 (FTP)	**Inbound**: Unencrypted or Encrypted (Explicit SSL) TCP connections for transferring files with EFT via FTP protocol used by FTP clients. **Outbound**: Unencrypted or Encrypted (Explicit SSL) TCP connections used by EFT to transfer files via FTP protocol with other FTP servers.
TCP: 990/ (FTP Implicit SSL) TCP: 989 (outbound)	**Inbound**: Encrypted TCP connections for transferring files with EFT via FTP protocol used by FTP clients. **Outbound**: Encrypted TCP connections used by EFT to transfer files via FTP protocol with other FTP servers.
TCP: 29000-30000 (FTP using PASV)	**Inbound**: Unencrypted or Encrypted TCP connections for transferring files with EFT via FTP when using PASV mode by FTP clients.

Ports	Purpose
EFT Management, Notifications, and Auditing and Reporting	
TCP: 1100 (administration Port)	TCP Unencrypted or Encrypted (SSL/TLS) connection used by EFT to manage its configuration via EFT administrator console or SFTPCOMInterface API
TCP: 4450 (HTTPS)	Port used by EFT for REST API.
TCP: 1433 (SQL Server)	TCP Unencrypted or encrypted (SSL/TLS) connection used to save and retrieve ARM logs into SQL Server
TCP: 1521 (Oracle) TCP: 2484 (Oracle SSL)	TCP Unencrypted or encrypted (SSL/TLS) connection used to save and retrieve ARM logs into SQL Server
TCP: 25,465, 587 (SMTP)	TCP unencrypted connections used by EFT protocol for sending email notifications via SMTP.
TCP: 143 (IMAP) TCP: 993 (IMAP SSL)	TCP unencrypted or encrypted (SSL) connections used by EFT for sending email notifications via IMAP.
EFT Content Integrity Control	
TCP: 1344 (ICAP)	Unencrypted or encrypted (SSL/TLS) HTTP connection used by EFT to communicate with an ICAPserver protocol for DLP (e.g. virus scanning, content filtering).
DMZ Gateway	
UDP: 8443	Port used by DMZ gateway to connect to another DMZ using FAST protocol for file transfers using the accelerate transfer module.
TCP: 44500	TCP Unencrypted or encrypted (SSL/TLS) connections used by EFT to connect to, control DMZ and transfer files from DMZ gateway.
Storage	
Direct TCP: 445 NetBIOS UDP: 137,138 NetBIOS TCP:138,139	SMB/CIFS protocol used by EFT to connect to a file shares (NAS) as a backend data storage
TCP: 860, 3260	iSCSI ports typically used by SAN storage, and consumed by EFT as storage presented as a NTFS local drive or file shares.
UDP: 138	DFS, Group Policy and NetBIOS used for Storage replication if used by EFT Server

Ports	Purpose
EFT High Availability	
TCP: 1801 RPC: 135, 2101*, 2103*, 2105* UDP: 3527, 1801	Message Queuing default ports used by EFT to operate when deployed in High Availability mode and maintain its configuration synchronized and load balance processing of event rules. UDP ports used when EFT is configured as multicast.
Active Directory	
Active Directory TCP: 135	RPC protocol used by Microsoft for Active Directory replication
UDP: 67	DHCP Server
TCP 139	User and Computer Authentication, Replication, DFSN, NetBIOS Session Service, NetLogon
TCP and UDP: 53	User and Computer Authentication, Name Resolution, Trusts
LDAP	
TCP and UDP: 389	LDAP Directory, Replication, User and Computer Authentication, Group Policy, Trusts
TCP: 636	LDAP SSL Directory, Replication, User and Computer Authentication, Group Policy, Trusts
TCP: 3268	LDAP Global catalog for Directory, Replication, User and Computer Authentication, Group Policy, Trusts
TCP:3269	LDAP Global catalog for Directory, Replication, User and Computer Authentication, Group Policy, Trusts
Advanced Authentication	
TCP: 1812	RADIUS server default port used by EFT for multifactor authentication
TCP: 4400 (HTTPS)	Encrypted HTTPS connections used by EFT to authenticate users with the Identity Provider Server using SAML protocol

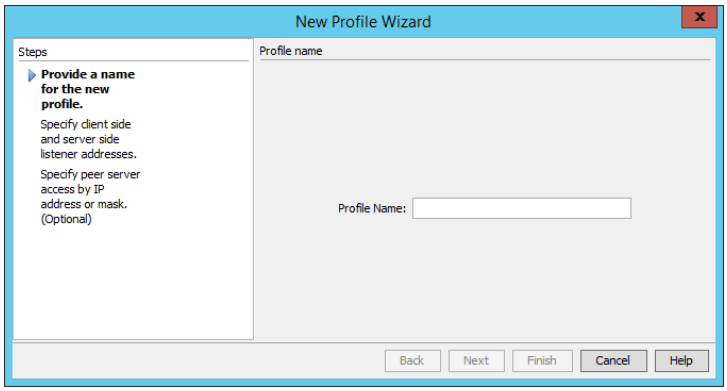
Creating a DMZ Gateway Profile

Creating a DMZ Gateway Profile includes specifying the listening IP address for incoming clients, specifying the listening IP addresses and port for the connecting application, and specifying the IP addresses that are allowed or denied access.

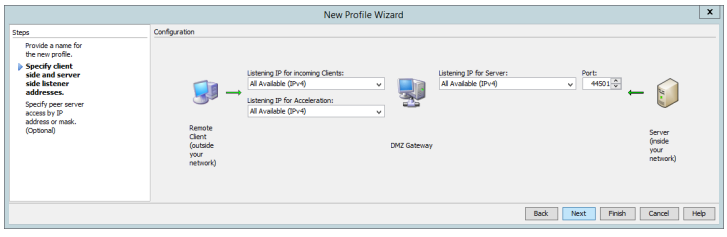
To create a Profile

1. Do one of the following:
   - Right-click in the **Profiles**tree, then click **New Profile**.
   - On the toolbar, click **New Profile**.
   - On the main menu, click **Profile > New**.

   The **New Profile Wizard** appears.



2. In the **Profile Name**box, provide a unique name for this Profile. The name will appear in the interface, logs, error messages, and reports.
3. Click **Next**. The **Configuration** page of the wizard appears.



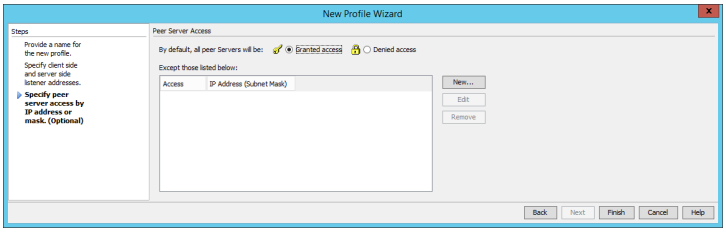
4. In the **Listening IP for incoming Clients** box, click the down arrow to select one or more IP addresses for incoming clients.
5. In the **Listening IP for Server** box, click the down arrow to select one or more listening IP addresses for the server.

> **NOTE:** Refer to Specifying the Listening IP Addresses for details.

6. In the **Port**box, provide the port number over which connections are allowed.

   > **NOTE:** The connection will be refused if the IP address is on the IP address ban list.

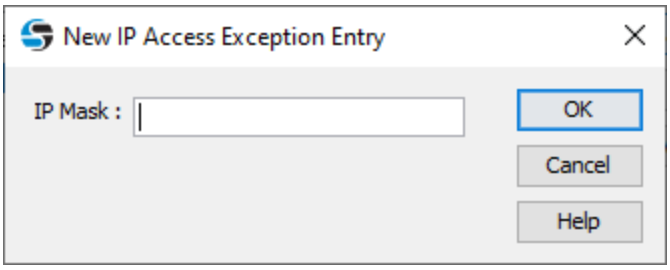
7. If you are using the Accelerate module in EFT, specify the **Listening IP for Acceleration**.
8. Click **Next**. The **Peer Server Access** page appears.



9. All IP addresses are granted access by default. To grant or deny access to specific IP addresses (optional):
10. Click **Granted access** or **Denied access**.
    - If most IP addresses are *allowed* access, click **Granted access**, then add the exceptions.
    - If most IP addresses are *denied* access, click **Denied access**, then add the exceptions.

      For example, if you want to allow only 192.168.174.159 and block every other IP address, click **Denied access**, click **Add**, then type `192.168.174.159`in the **IP Mask** box. This will deny access to all IP addresses except 192.168.174.159.

11. Click **New**. The **New IP Access Exception Entry** dialog box appears.



12. Specify the IP address or range of IP addresses to which you are denying or granting access. You can use wildcards to select ranges of IP addresses.
13. Click **OK** to close the **New IP Access Exception Entry** dialog box.
14. Click **Finish**. The IP Mask appears in the exception list.

Deleting a Profile

You can configure multiple Profiles. You can delete Profiles that you no longer use, but you cannot delete a Profile if it is the only Profile.

To delete a Profile

- Click the Profile in the tree, then do one of the following:
  - Right-click the Profile name, then click **Delete Profile**.
  - On the toolbar, click **Delete Profile**.
  - On the main menu, click **Profile > Delete Profile**.

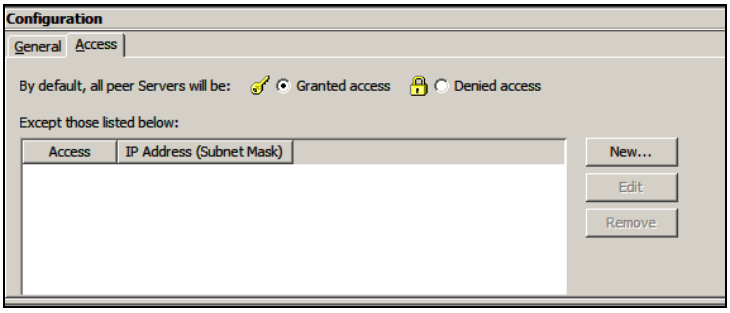
The Profile is deleted from the tree.

Editing a Profile

When you create a new Profile, you define the listening IP address for remote connecting clients, the listening IP address and port for the server inside your network, and any IP addresses exceptions. After the Profile is created, you can edit the Profile's configuration as necessary. You can also rename or delete the Profile. When you make a change to a Profile, before you click **Apply**, an asterisk appears in the tree next to the Profile that you are editing. You must define a unique IP address/port combination for each Profile.

To edit a Profile

1. In the **Navigation** pane, click the Profile that you want to edit.
2. In the **Configuration** pane, click the **General** tab.
3. Specify the **Listening IP for incoming Clients** box and the **Listening IP for Server**. Refer to Specifying the Listening IP Addresses for detailed information.
4. In the **Port** box, provide the port number over which connections are allowed.
5. In the **Configuration** pane, click the **Access** tab.



6. Specify the IP addresses or IP mask of servers that are allowed or denied access.
7. In the toolbar, click **Apply Changes**. If the IP address and port are not unique, an error message appears; otherwise, the DMZ Gateway will allow the server to connect.

If you have made multiple edits, you can revert to the last-saved state by clicking **Revert Changes** (undo) before clicking **Apply Changes**. However, once you click **Apply Changes**, you cannot go back.

Renaming a Profile

The Profile name appears in statistics, logs, messages, and reports. You can change the name in the DMZ Gateway interface.

To change the name of a Profile

1. Click the Profile in the tree, then do one of the following:
    - Click the Profile name again.
    - Right-click the Profile name, then click **Rename Profile**.
    - On the toolbar, click **Rename Profile**.
    - On the main menu, click **Profile > Rename**.

    The name in the tree becomes editable.
2. Type a new name for the tree, then press ENTER.

DMZ Gateway Components

DMZ Gateway consists of the following components:

- The main server component, the DMZ Gateway Server
- A launch and monitoring component, the DMZ Gateway Server Service
- A configuration and monitoring component, the DMZ Gateway administration interface

DMZ Gateway Server

The DMZ Gateway Server is the main Java-based functionality. An embedded Java Runtime Environment (JRE) is used to execute this functionality. Refer to Updating the JRE for DMZ Gateway for detailed information about updating the JRE.) The DMZ Gateway Server component is never executed directly, but rather controlled and monitored using the DMZ Gateway Server Service component.

DMZ Gateway Server Service

The DMZ Gateway Server Service component is responsible for properly initializing the JRE and launching the DMZ Gateway Server component. It then stays resident and provides watchdog monitoring functionality over the DMZ Gateway Server component. It also provides logging and diagnostic capabilities to facilitate troubleshooting any possible issues that may occur during server startup. (Refer to DMZ Gateway Logging for detailed information.)

DMZ Gateway Administration Interface

The DMZ Gateway administration Interface is a Java-based thick client that provides graphical administration capabilities for the DMZ Gateway Server. The interface communicates with the DMZ Gateway Server via a local-only TCP/IP administration port.

The administration capabilities include:

- Creating and Configuring Profiles
- Viewing Statistics
- Controlling the Server Service/Daemon

DMZ Gateway System Files

The following file names can be observed when running DMZ Gateway:

On Windows Systems:

- In the Windows Services dialog box:
  - **DMZ Gateway Server** is the DMZ Gateway service.
- In the **Task Manager**:
  - **DMZGatewayServerService.exe** launches and monitors the DMZ Gateway Server.
  - **DMZGatewayServer.exe** is the DMZ Gateway Server.
  - **DMZGatewayadministrator.exe** is the administration interface.

On Non-Windows Systems:

- **dmzgatewayd** is the DMZ Gateway daemon.
- **DMZGatewayServer** is the DMZ Gateway Server.
- **DMZGatewayadministrator** is the DMZ Gateway administration interface.

You can view all running DMZ Gateway executables by typing:

```
ps -ef | grep DMZGateway
```

DMZ Gateway Headless Administration

Configuration and administration of the DMZ Gateway is typically performed using the DMZ Gateway administration interface. This interface runs local to the DMZ Gateway Server and uses a local-only TCP/IP connection to configure the DMZ Gateway Server and to obtain status and statistical information. Administrators of headless systems have the following options for configuring and monitoring the DMZ Gateway:

- Use a remote X11 server to display the administration interface
- Manually configure and monitor the DMZ Gateway Server through the file system

X11 Server Method

While the exact steps required to display the administration interface remotely may differ from system to system, the following steps are typical:

1. Ensure the X11 Server is running on the host system on which the user interface will be displayed.
2. Allow the DMZ Gateway computer access to the X11 Server using the xhost command. For example, issuing the following command in a terminal window on the host system will allow access to all incoming IP addresses:

   ```
   xhost +
   ```
3. Log in to the DMZ Gateway computer as a user with the appropriate permissions to run the DMZ Gateway administration interface.
4. Export the display to the host X11 server by issuing the following command in a terminal window:

   ```
   EXPORT DISPLAY=<Host IP>:0.0
   ```
5. Execute the DMZ Gateway administration Interface script in a terminal window:

   ```
   <Installation Directory>/bin/DMZGatewayadministrator
   ```

   For example:

   ```
   /opt/dmzgateway/bin/DMZGatewayadministrator
   ```

Note that some Unix-based installations come preconfigured in a pure headless fashion and may lack the necessary X11 libraries required to display the administration interface remotely. Please consult your operating system documentation for information on installing the necessary libraries.

Manual Configuration Method

The DMZ Gateway Server may be configured by manually editing the DMZ Gateway Configuration file **gwconfig.xml**. For details on the configuration file, refer to DMZ Gateway Server Configuration File Reference.

It is highly recommended that the configuration be edited while the DMZ Gateway Server is ***not***running; changes made to the configuration file will not take effect until the DMZ Gateway Server is restarted.

DMZ Gateway Logging

All logging functionality in DMZ Gateway comes preconfigured with the optimal settings. The information below is provided to help you understand what is in the logs. When necessary, modifying the configuration for the logging functionality should only be performed with the aid of Globalscape Customer Support.

The following logs are created and populated during the operation of DMZ Gateway:

- DMZ Gateway Communications Activity Log (**DMZActivity.log**)
- DMZ Gateway Server Diagnostics Log (**DMZGatewayServer.log**)
- DMZ Gateway Server Service Diagnostics Log (**DMZGatewayServerService.log**)
- DMZ Gateway Statistics Log (**DMZStatistics.log**)
- DMZ Gateway Server Event Viewer (Windows Operating Systems Only)
- DMZ Gateway Server Syslog(Solaris/Linux-based Operating Systems Only)

DMZ Gateway Communications Activity Logging

The DMZ Gateway communications activity logging records messages relating to communications to a W3C Extended Log File-formatted file. By default, this log file is created as **<installation directory>\logs\DMZActivity.log**. The format of the log file consists of a header at the beginning of the file and subsequent lines for each communications message generated by the DMZ Gateway Server. (Not all fields will be populated for every message. More information on the W3C Extended Log File format is available on the W3C Web site at http://www.w3.org/TR/WD-logfile.html.)

(The examples below are for illustration only and do not necessarily reflect your version or installation of DMZ Gateway.)

The header is of the format:

```
#Software: DMZ Gateway Server Version: 3.0.0 build 4

#Version: 3.0

#Date: 2009-09-28 07:31:48

#Fields: time status rs-ip rs-comment s-ip s-comment c-ip
 c-comment
```

where:

- Software – Identifies the application that generated the log file. In this case, the DMZ Gateway Server. This line will also contain the application version and build number of the DMZ Gateway Server.
- Version – The version of the extended log file format used.
- Date – The date and time the log file was initially created.
- Fields – The field names for the fields included in each log message. The fields are defined as:
    - time – The date and time the log message was generated
    - status – The status of the message where a value of 0 indicates a failure or error and a value of 1 indicates success.
    - rs-ip – The remote server IP Address and Port number. This represents the peer server connected to the Peer Notification Channel. This will typically be the EFT.
    - rs-comment – Textual status message related to the remote server.
    - s-ip – The server IP Address and port. This represents the DMZ Gateway Server.
    - s-comment – Textual status message related to the DMZ Gateway Server.
    - c-ip – The client IP Address and port. This represents the FTP client connection.
    - c-comment – Textual status message related to the client.

The verbosity of messages written to the communications activity log is configurable via the DMZ Gateway administration interface. By default, verbose logging is not enabled. When set to false, only basic communications initialization and de-initialization messages are logged to the activity log. This includes messages concerning Peer Notification Channel listener startups and stops. When verbose logging is enabled, additional communications messages concerning client connections are logged.

Essentially, messages that may occur throughout the course of operating the DMZ Gateway Server are governed by the "Verbose Activity Logging" setting whereas messages that only occur during initial startup and shutdown are always logged. The DMZ Gateway Server appends the log during each run of the DMZ Gateway Server.

The log file will automatically archive itself when reaching 10 MB in size and maintains the last 10 log files in the form **DMZActivity.<X>**where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Server Diagnostics Logging

The DMZ Gateway Server diagnostics logging functionality provides diagnostic-level messages for the operation of the DMZ Gateway Server. This diagnostic information may be used to identify errors, warnings, and other information of interest that occur during the operation of the DMZ Gateway Server.

By default this functionality logs to the file **<installation directory>\logs\DMZGatewayServer.log**.

The DMZ Gateway Server appends the log during each run of the DMZ Gateway administration interface. The log file automatically archives itself when reaching 10 MB in size and maintains the last 10 log files in the form **DMZGatewayadministrator.<X>** where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

Appenders

Appenders can be edited in the **\Program Files\GlobalSCAPE\DMZ Gateway\confserver_log_config.xml** file to set parameters such as the DMZGatewayServer.log file-naming pattern (default is `DMZGatewayServer-03- 07-2022-1.log`), bufferedIO, DefaultRolloverStrategy, SizeBasedTriggeringPolicy, set globally at the top of the file, and others.

DMZ Gateway Server Service Diagnostics Logging

This logging records diagnostic information generated by the DMZ Gateway Server service executable. The diagnostic information may be used to identify errors or warnings that occur during startup of the DMZ Gateway Server. By default, this functionality logs to the following file:

<installation directory>\logs\DMZGatewayServerService.log.

The DMZ Gateway Server appends the log during each run of the DMZ Gateway Server. The log file automatically archives itself when it reaches 10 MB in size and maintains the last 10 log files in the form **DMZGatewayServerService.log.<X>** where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Statistics Logging

Statistics logging is disabled by default, because statistics are typically viewed through the DMZ Gateway administration interface. When enabled, this functionality records various statistical data in CSV format to the log file **<installation directory>\logs\DMZStatistics.log**. A header row is generated at the beginning of each file and then data rows are periodically added for each Profile/Peer Server connection.

The statistical data includes the following fields:

- Timestamp – the date and time the row was generated
- Profile – the Profile to which the row of statistical data pertains
- Server – the Peer Server (e.g. EFT) to which the row of statistical data pertains
- Client Received (B) – the total number of bytes received from clients for the specified Profile/Server.
- Client Sent (B) – the total number of bytes sent to clients for the specified Profile/Server.
- Server Received (B) – the total number of bytes received from the Server for the specified Profile/Server.
- Server Sent (B) – the total number of bytes sent to the Server for the specified Profile/Server.
- Client Receive Rate (Bps) – the number of bytes per second received from clients for the specified Profile/Server.
- Client Send Rate (Bps) – the number of bytes per second sent to clients for the specified Profile/Server.
- Server Receive Rate (Bps) – the number of bytes per second received from the Server for the specified Profile/Server.
- Server Send Rate (Bps) – the number of bytes per second sent to the Server for the specified Profile/Server.
- Connections Accepted – the total number of connections allowed for the specified Profile/Server.
- Connections Refused – the total number of connections refused for the specified Profile/Server.

The log is appended during each run of the DMZ Gateway service. The log file automatically archives itself when reaching 10 MB in size and maintains the last 10 log files in the form **DMZGatewayServerService.log.<X>**where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Server Event Viewer (Windows Operating Systems Only)

On Windows operating systems, DMZ Gateway records significant events to the Windows Event Log. Events originating from the DMZ Gateway are recorded in the Application Event Log and by default include the following types of events:

- DMZ Gateway Service start
- DMZ Gateway Service stop
- DMZ Gateway Service restart
- DMZ Gateway Service startup failures
- All FATAL and ERROR level diagnostic log messages recorded in the DMZ Gateway Server Diagnostics Log

Additionally, the startup and shutdown activities originating from the Windows Service Control Manager are recorded in the System Event Log.

DMZ Gateway Server Syslog (Solaris/Linux-based Operating Systems Only)

On Solaris and Linux-based operating systems, DMZ Gateway can record significant events in the local Syslog. By default, messages will be logged with an indent of “DMZ Gateway Server” to the LOG_USER facility and include the LOG_PID option. (Refer to http://www.kernel.org/doc/man-pages/online/pages/man3/syslog.3.htmlfor information on the syslog functionality or type “man syslog” in a terminal window.)

On Solaris systems, it may be necessary to configure the syslog daemon to include logging of the LOG_USER facility. Typically, you can edit the **/etc/syslog.conf** file as root and add a line such as:

```
user.info <tab> /var/administrator/message
```

Replace <tab> with an actual TAB character. This will instruct the syslog daemon to log LOG_USER facility messages to the **/var/administrator/message**log file. After saving your changes, you will need to restart the syslog daemon as root with a command such as:

```
svcadm restart system-log
```

DMZ Gateway Administration Interface Logging

The following log files are created and populated during the operation of the DMZ Gateway administration interface:

- DMZ Gateway Administrator Diagnostics Logging
- DMZ Gateway Administrator Launcher Diagnostics Logging

DMZ Gateway Administration Diagnostics Logging

The DMZ Gateway administration diagnostics logging provides diagnostic-level messages for the operation of the DMZ Gateway administration interface. This diagnostic information may be used to identify errors or warnings that occur during the operation of the administration interface.

By default this functionality records to the file:

<installation directory>\logs\DMZGatewayadministrator.log

The log is appended during each run of the DMZ Gateway administration interface. The log file automatically archives itself when reaching 10 MB in size and maintains the last 10 log files in the form **DMZGatewayadministrator.<X>**where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Administrator Launcher Diagnostics Logging

This logging records diagnostic information generated by the DMZ Gateway administrator Launcher executable, **<installation directory>\bin\DMZGatewayadministratorLauncher(.exe)**. This executable is responsible for starting the Java Virtual Machine and launching the DMZ Gateway administration interface. The diagnostic information may be used to identify errors or warnings that occur during startup of the administration application. By default this functionality logs to the file **<installation directory>\logs\DMZGatewayAdminLauncher.log**. This file is overwritten during every execution of the utility.

DMZ Gateway Server Configuration File (gwconfig.xml) Reference

The DMZ Gateway Server configuration file, **gwconfig.xml**, contains the main configuration settings governing communications through the DMZ Gateway Server.

The configuration file is in XML format and its contents are verified against a document type definition (DTD) file **gwconfig.dtd**.

Typically, the configuration items specified in **gwconfig.xml**will be edited via the DMZ Gateway administration interface. However, it is possible to edit the configuration settings using a text editor. Additionally, some advanced configuration items are not available via the DMZ Gateway administration interface and thus will require manual editing to configure.

Changes made to the configuration via manual editing will not take effect until the DMZ Gateway Server is restarted. Thus, the following steps should be followed:

1. Stop the DMZ Gateway Server service.
2. Edit the **gwconfig.xml**file using a text editor.
3. Save changes to the file.
4. Start the DMZ Gateway Server service.
5. Verify the DMZ Gateway Server has started and verify that no ERROR or FATAL messages are present in the DMZGatewayServer.logdiagnostics log file.

Configuration Validation

During startup, the DMZ Gateway Server will load the configuration file and validate its structure against the definition in the DTD file. It will also validate the various data constraints governing each element. If the configuration file format is invalid or the configuration violates any constraints, the DMZ Gateway Server will log an appropriate error message in the diagnostics log DMZGatewayServer.logand shut down.

Configuration Elements

Please refer to the DTD file for the valid structure of the configuration file. The following describes the configuration elements available in the **gwconfig.xml** file.

- **ConfigurationVersion**

  The internal version number used to track the configuration file format. ***Do not edit.***

- **AdminPort**

  The DMZ Gateway administration interface communicates with the DMZ Gateway Server via a local-only TCP/IP communications port to conduct administrative tasks. This configuration item specifies the port to use for this communication path. This setting is not configurable via the user interface and must be edited manually.

  Valid values: 0 to 65525.

  Setting the port to 0 instructs the operating system to randomly select an available port from its ephemeral port range.

  Setting the port to 1 through 65535 specifies an exact port. Care should be taken to ensure the specified port is not in use on the system.

  Default value: 0

- **AdminPortEnabled**

  The DMZ Gateway administration interface communicates with the DMZ Gateway Server via a local-only TCP/IP communications port to conduct administrative tasks. This configuration item allows the user to disable this communication path. Note that disabling the administration port will prevent use of the DMZ Gateway administration Interface. The DMZ Gateway Server inherently only allows local connections via the administration port. This setting provides an additional level of security by allowing the operator to disable the administration port altogether once initial configuration has been completed. This setting is not configurable via the user interface and must be edited manually.

  Valid values:

  true - enable the administration port.

  false – disable the administration port.

  Default value: true

- **VerboseLoggingEnabled**

  Enables or disables verbose log messages in the DMZ Gateway Server communications activity log file, DMZActivity.log. This setting is configurable via the user interface.

  Valid values:

true - enable verbose log output

false – disable verbose log output

Default value: false

- **GlobalPNCKeepalivePeriod**

  When a Peer Server application, such as the EFT, is connected to the DMZ Gateway Server via a Peer Notification Channel, keepalive functionality is used to verify that the communications channel is valid and alive. The keepalive functionality verifies the validity of the channel by periodically sending a message to the peer server and verifying that it receives a reply. This setting governs how often this check is performed for all Profiles. This setting is not configurable via the user interface and must be edited manually.

  Valid values: 1 to 2^63 – 1, in milliseconds

  Default value: 30000
  (30 seconds)

- **StatisticsLoggingEnabled**

  The DMZ Gateway Server is capable of periodically logging statistical information to a statistics log file. This setting enables this logging functionality. This setting is not configurable via the user interface and must be edited manually.

  Valid values:

  true - enable statistics logging

  false – disable statistics logging

  Default value: false

- **StatisticsLoggingPeriod**

  This setting governs how often the current set of statistics within the DMZ Gateway Server is recorded in the statistics log file. This setting is not configurable via the user interface and must be edited manually.

  Valid values: 1 to 2^63 – 1, in milliseconds

  Default value: 300,000(5 minutes)

- **Profiles**

This element encloses 0 to 15 Profile elements. If no Profiles are specified in the configuration file, the DMZ Gateway Server will automatically create a default Profile during startup. If more than 15 Profiles are defined, the DMZ Gateway Server will log the error during startup and subsequently shut down.

- **Profile**

  This enclosing element contains the configuration items defining a Profile. Profiles are configurable via the administration interface.

- **ProfileName**

  This is the name of the enclosing Profile. The name must be unique among all defined profiles. If the name is not unique, the DMZ Gateway Server will log the error during startup and subsequently shut down. Profile Names are configurable via the administration interface.

  Valid values: From 1 to 260 alphanumeric characters.

  Default value: Profile

- **ServerIP**

  This the IP Address of a local network adapter on which to listen for connections from peer servers on a peer notification channel. Server Listener IPs are configurable via the administration interface.

  Valid values: All or a specific IP address. When "All" is specified, the DMZ Gateway Server will listen on all IP address/port combinations on the local computer that are not already in use.

  Default value: All

- **ServerPort**

  This is the port to use with the IP address(es) specified in the ServerIP element to fully define the IP Address:Port combination on which to listen for connections from peer servers. Server listener ports are configurable via the administration interface.

  Valid values: 0 to 65535. When set to 0 the operating system will randomly select an available port from its ephemeral port range

  Default value: 44500

- **ClientIP**

This the IP address of a local network adapter on which to listen for connections from clients. Client Listener IPs are configurable via the administration interface.

Valid values: All or a specific IP address. When "All" is specified, the DMZ Gateway Server will listen on all IP address/port combinations on the local computer that are not already in use.

Default value: All

- **PNCKeepalivePeriod**

  This element allows optional overriding of the GlobalPNCKeepalivePeriod on a per-Profile basis. This setting is not configurable via the user interface and must be edited manually.

  Valid values: 1 to 2^63 – 1, in milliseconds

  Default value: 30000 (30 seconds)

- **NetworkAccessPolicy**

  This enclosing element contains the configuration settings for the IP access policy used to validate connections to the Peer Notification Channels of the enclosing Profile. The Network Access Policies for each Profile are configurable via the administration interface.

- **DefaultAccessPolicy**

  This is the policy to use by default when validating connections to the Peer Notification Channels of the enclosing Profile. The Default Access Policy for each Profile is configurable via the administration interface.

  Valid values:

  Grant – by default all connections will be granted access.

  Deny – by default all connections will be denied access.

  Default value: Grant

- **GrantPolicyExceptions**

  This element encloses 0 or more Exception elements that act as exceptions to the Grant All policy. Thus, they define what will be denied access. A maximum of 100 Exception elements may be defined. If more than 100 are defined, the

DMZ Gateway Server will log the error during startup and subsequently shut down. The Grant Policy Exceptions for each Profile are configurable via the administration user interface.

- **DenyPolicyExceptions**

  This element encloses 0 or more Exception elements that act as exceptions to the Deny All policy. Thus, they define what will be granted access. A maximum of 100 Exception elements may be defined. If more than 100 are defined, the DMZ Gateway Server will log the error during startup and subsequently shut down. The Deny Policy Exceptions for each Profile are configurable via the administration user interface.

  Exception

  This element defines an exception to the enclosing Policy type. Exceptions are implemented as IP address masks that allow definition of masks that may be used to match the IP Address of a connecting peer server. The exceptions are configurable via the administration interface.

  Valid values: IP Address Masks match against IPv4 or IPv6 IP addresses

File Location

For new installs, the configuration file is created the first time the DMZ Gateway Server is started. When the configuration file is created, the corresponding DTD file is also created. By default, the configuration and DTD files are created in the DMZ Gateway installation directory. However, to facilitate sharing of configuration data in high availability clustered installs, an alternate shared data location may be specified.

Shared Configuration Location

An alternate shared data location may be specified either during the installation process or by subsequently editing the **DMZGatewayServerService.conf**file.

To specify the shared data location:

1. Stop the DMZ Gateway Server Service/Daemon.
2. Edit the **<Installation Directory>\conf\DMZGatewayServerService.conf**file using your preferred text editor.
3. Locate the following line in the file:

   ```
   set.DMZ_SHARED_CONFIG_DIRECTORY=""
   ```
4. Edit the line and enter the shared data location within the quotes, for example:

```
On Windows: set.DMZ_SHARED_CONFIG_
DIRECTORY="\\jupiter\DataShare\DMZGateway"
On Solaris/Linux: set.DMZ_SHARED_CONFIG_
DIRECTORY="/export/share/dmzgateway"
```

5. Save the changes to the file.
6. If you want to reuse the settings in the existing **gwconfig.xml**configuration file, move the file to the new location.
7. Start the DMZ Gateway Server Service/Daemon.

Please ensure that the operating permissions governing the DMZ Gateway Server service/daemon are set such that the process is able to access the specified shared configuration directory.

Note that the DMZ Gateway Server will automatically (re)generate the **gwconfig.dtd** DTD file in the specified shared data location. Additionally, for convenience, the file will also be generated in the installation directory.

DMZ Gateway Server Unix/Solaris Daemon

On Solaris and Linux-based system, the DMZ Gateway Server is started and controlled using the system daemon script **<Installation Directory>/bin/dmzgatewayd**. When necessary, this script will call the Java Service Wrapper utility **<Installation Directory>/bin/DMZGatewayServerServic**e to start and stop the **DMZGatewayServer** Java executable.

Per convention, if the user opted to register the service with the operating system during installation, a symbolic link **/etc/init.d/dmzgatewayd**will have been created. This symbolic link points to the **<Installation Directory>/bin/dmzgatewayd** script. Additionally, the appropriate symbolic links will have been created in the **/etc/rc.d** directories so that the DMZ Gateway Server will be started and stopped appropriately during system startup and shutdown.

You can control the system daemon by executing either /**etc/init.d/dmzgatewayd**or **<Installation Directory>/bin/dmzgatewayd**. The script accepts a set of command line options. Running the script without any command line options will display the set of available options, which are itemized below:

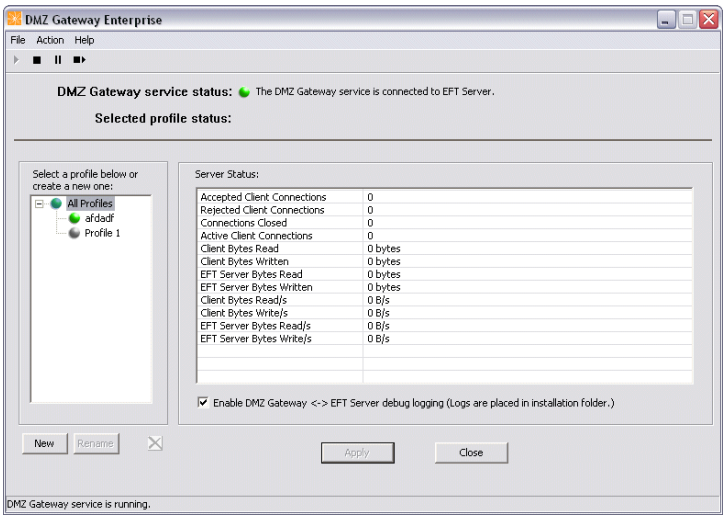
- console – Runs the DMZ Gateway Server as a console program as opposed to a system daemon.
- start – Starts the DMZ Gateway Server as a daemon process
- stop – Stops the DMZ Gateway Server daemon process, if running.
- restart – Stops the DMZ Gateway Server daemon process, if running, and then starts it.
- condrestart – Restarts the DMZ Gateway Server daemon process if it is currently running.
- status – Indicates if the DMZ Gateway Server daemon process is currently running or not.
- dump – Instructs the Java Virtual Machine to log the state of all active threads to the log.

DMZ Gateway Status

The top pane of the DMZ Gateway interface displays the DMZ Gateway service status and the selected profile's status. The pane displays:

- When DMZ Gateway service is stopped.
- When DMZ Gateway service is running but no Site is connected to the selected profile.
- When DMZ Gateway service is running and there is a Site connected to the profile and a port is assigned.
- When DMZ Gateway service is running and there is a Site connected to the profile, but no port is assigned.

When the **All Profiles** node is selected, as shown below, the **Server Status** area displays the size of items transferring through DMZ Gateway. (Because **All Profiles** is selected, no status appears in the Selected profile status area.)



Server statistics include:

- Accepted Client Connections - Count of client connections accepted through the DMZ Gateway during the current run of the DMZ Gateway
- Rejected Client Connections - Count of client connections rejected through the DMZ Gateway during the current run of the DMZ Gateway

- Connections Closed - Count of connections closed during the current run of the DMZ Gateway
- Active Client Connections - Count of the currently active client connections
- Client Bytes Read - Number of bytes received from Clients
- Client Bytes Written - Number of bytes sent to Clients
- EFT Server Bytes Read - Number of bytes received from Servers
- EFT Server Bytes Written - Number of bytes sent to Servers
- Client Bytes Read/s - Transmission speed when receiving from Clients in bytes per second (B/s)
- Client Bytes Written/s - Transmission speed when sending to Clients in bytes per second (B/s)
- EFT Server Bytes Read/s - Transmission speed when receiving from Servers in bytes per second (B/s)
- EFT Server Bytes Written/s - Transmission speed when sending to Servers in bytes per second (B/s)

When the **All Profiles** node is selected, a check box appears at the bottom of the right pane that allow you to enable or disable debug logging.

Routing AS2 Traffic through DMZ Gateway

You can configure Event Rules to cause AS2 traffic to route through the DMZ Gateway using the **AS2 Send file to host** Action. You can use the **AS2 Send File to host** Action in the Folder Monitor, Timer, and all file-based Events.

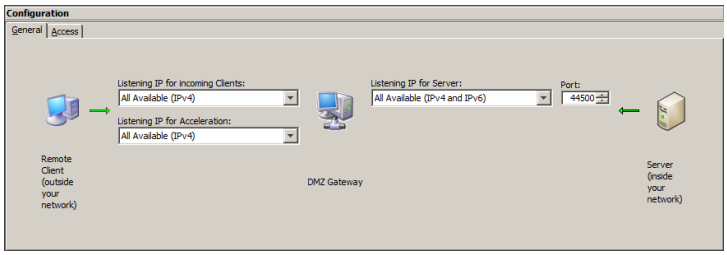
To route AS2 traffic through DMZ Gateway

1. Create a new Event Rule, such as a File Uploaded event. (If necessary, refer to "Creating Event Rules" in the EFT Server documentation.)
2. Add the **AS2 Send file to host** Action to the Rule, then click the file or host link. The **AS2 Send File** dialog box appears.
3. In the **AS2 Send File** dialog box, specify trading partner profile to use or define the trading partner options.
4. Add the **Copy/Move File to Host** Action to the Rule.

5. In the **Rule** pane, click one of the undefined parameters (for example, '%FS.PATH%'). The **Offload Action Wizard** appears.
6. Follow the instructions in Using DMZ Gateway as an Outbound Proxy to define the Rule.

Specifying the Listening IP Addresses

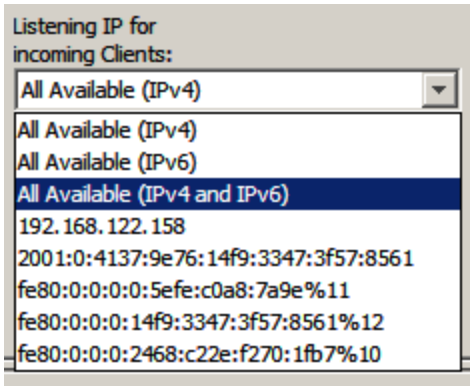
For each DMZ Gateway Profile, you specify 2 IP addresses:



1. One address is used by client programs to connect. This is typically an external-facing address. When a Site configured at a peer server connects to the DMZ Gateway over the PNC, the DMZ Gateway reads the list of client ports configured in the Site. These ports are then combined with the client IP Address and it is on these client IP address/Site port combinations that the DMZ Gateway will listen for client connections.
2. The other address specifies the IP address on which to listen for connections from peer servers. The communications established using this address is known as the *Peer Notification Channel* or *PNC*. Typically, this IP Address will be an internal-facing address. This address is combined with the configured port value and it is on this IP Address/port combination that the DMZ Gateway will listen for connections from peer servers.

   If you are using the Accelerate module in EFT, you should also specify the Listening IP for Acceleration.

   Each address is configured by selecting the IP address to use from a drop-down list. The list of IP addresses includes all IPv4 and IPv6 addresses present on the computer. Additionally, the list includes an **All Available** setting for both IPv4 and IPv6. (IPv6 connections to DMZ Gateway are not supported on Windows Server 2003.)



3. In the **Listening IP for incoming Clients** box, click the down arrow to select one or more IP addresses for incoming clients. (Only the IP addresses defined on this computer appear in this box.) You can specify:
    - **All Available (IPv4)**—Listen for client connections on all IPv4 addresses.
    - **All Available (IPv6)**—Listen for client connections on all IPv6 addresses.
    - **All Available (IPv4 and IPv6)**—Listen for client connections on all IPv4 and IPv6 addresses.
    - **A specific IP address**—Listen for client connections on all on a specific IP address.
4. In the **Listening IP for Server** box, click the down arrow to select one or more listening IP addresses for the server. (Only the IP addresses defined on this computer appear in this box.) **All Available** means that DMZ Gateway will listen on the IP address/port combination ONLY IF that IP address/port combination is not already being used by another Profile. Profiles configured with an explicit IP address have precedence over Profiles configured with **All Available**. You can specify:
    - **All Available (IPv4)**—Listen for server connections on all IPv4 addresses.
    - **All Available (IPv6)**—Listen for server connections on all IPv6 addresses.
    - **All Available (IPv4 and IPv6)**—Listen for server connections on all IPv4 and IPv6 addresses.
    - **A specific IP address**—Listen for server connections on all on a specific IP address.

IMPORTANT: **All Available**means that DMZ Gateway will listen on the IP address/port combination ONLY IF that IP address/port combination is not already being used by another Profile. Profiles configured with an explicit IP address have precedence over Profiles configured with **All Available**.

What Does This Mean for the Peer Server Listeners?

Suppose you have three IP addresses on the computer: IP 1, IP 2, and IP 3, and you have two Profiles: Profile 1 and Profile 2.

- Both Profiles are configured to use the same Peer Server Listener Port 54321.
- Profile 1 is set to use **All Available**.
- Profile 2 is set to use IP 2.

Profile 1 will listen on **IP 1:54321**and **IP 3:54321**, and Profile 2 will listen on **IP 2:54321**.

Now, suppose you delete Profile 2, making **IP 2:54321** available. The DMZ Gateway will detect this and update the communications listeners so that Profile 1 will now listen on **IP 1:54321**, **IP 2:54321**, and **IP 3:54321**.

What Does This Mean for the Client Listeners?

Suppose you have three IP addresses on the computer: IP 1, IP 2, and IP 3, and you have two Profiles: Profile 1 and Profile 2. Profile 1 is set to use **All Available** and Profile 2 is set to use IP 2.

Now suppose you have two Sites configured on EFT. Both Sites are configured to connect to the DMZ Gateway and use FTP port 21. Site 1 is set to connect to Profile 1, and Site 2 is set to connect to Profile 2.

Once both Sites are connected, the DMZ Gateway will establish client listeners for Site 1 on **IP 1:21**and **IP 3:21** (because Site 1 used Profile 1, which uses all available IP/port combinations not currently in use). For Site 2 the DMZ Gateway will establish a client listener on **IP 2:21**.

If Site 2 should disconnect for some reason (perhaps it was deleted), **IP 2:21** is now considered available. The DMZ Gateway will detect this and update the communications listeners so that Profile 1 will listen for client connections on **IP 1:21**, **IP 2:21**, and **IP 3:21**.

Related Topics

- Creating a Profile
- Editing a Profile

Starting and Stopping the DMZ Gateway Server Service

Typically, the DMZ Gateway server service is configured to start automatically when the computer is started. When the DMZ Gateway administration interface is launched, it determines whether the DMZ Gateway server service is running. If the DMZ Gateway server service is not running, a prompt appears asking if you want to start the DMZ Gateway service.

On Windows systems:

When you install DMZ Gateway, the service is configured to start automatically. You can start and stop the service in the Windows **Services**dialog box and in the DMZ Gateway administration Interface.

On non-Windows systems:

The installation script includes registering and starting the DMZ Gateway server daemon (configuring it to auto-start on system start and auto-stop on system stop). Alternatively, you can start and stop the server manually using the following commands:

```
<InstallDir>/bin/dmzgatewayd start

<InstallDir>/bin/dmzgatewayd stop
```

In the DMZ Gateway administration interface:

In the DMZ Gateway administration interface, you can start and stop the service from the Server menu or using the toolbar controls. The status of the DMZ Gateway server service appears in the status bar at the bottom of the interface. (for example, "DMZ Gateway is running.") You can start, pause, restart, or stop the DMZ Gateway service on the DMZ Gateway main menu or toolbar.

To start the DMZ Gateway

- On the DMZ Gateway main menu, click **Server >Start** or click **Start** on the toolbar.

To restart the DMZ Gateway

- On the DMZ Gateway main menu, click **Server > Restart** or click **Restart** on the toolbar.

To stop the DMZ Gateway

- On the DMZ Gateway main menu, click **Server > Stop** or click **Stop** on the toolbar.

DMZ Gateway Server PID Files

When the DMZ Gateway Server Service starts it will create the PID file **<Installation Directory>\DMZGatewayServerService.pid**. This file contains the process ID for the DMZ Gateway Server Service.

When the DMZ Gateway Server is started, the PID file **<Installation Directory>\DMZGatewayServer.pid** is created. This file contains the process ID for the DMZ Gateway Server.

DMZ Gateway Server Status Files

During the course of operation, the DMZ Gateway Server Service will create and update the status file **<Installation Directory>\DMZGatewayServerService.status**. This file will contain the current status of the DMZ Gateway Server Service. The possible contents are described at http://wrapper.tanukisoftware.org/doc/english/prop-statusfile.html.

During the course of operation the DMZ Gateway Server Service will create and update the status file <Installation Directory>\DMZGatewayServer.status. This file will contain the current status of the DMZ Gateway Server. The possible contents are described at http://wrapper.tanukisoftware.org/doc/english/prop-java-statusfile.html.

DMZ Gateway Server Monitoring

After starting the DMZ Gateway Server, the DMZ Gateway Server Service will stay resident and monitor the Server. If the Server crashes, the Service will wait 5 seconds and attempt to restart the Server.

Testing the Configuration

After you have installed DMZ Gateway, created and configured a Profile, and enabled DMZ Gateway in EFT, you can test your configuration by connecting to the server via DMZ Gateway and transferring a few files.

To test your configuration

Suppose your server is at IP address 192.168.174.176 and DMZ Gateway is at IP address 192.168.174.142, and you have configured DMZ Gateway in the server to allow connections over the HTTPS port 443.

1. Open a browser and in the address bar type `https://192.168.174.142`(the IP address of DMZ Gateway), then press ENTER.
2. You should be prompted to log in. Type the login credentials from a user defined on the server to which you want to connect.
3. Transfer a few files.
4. On the **Status**tab, you should see the numbers increase in the **Client Bytes Read**, **Client Bytes Written**, **Server Bytes Read**, and **Server Bytes Written** columns. Click **Refresh**, if necessary. (Note that if you connect to the server's IP address to transfer files, you are not going through the DMZ Gateway and, therefore, will not see any statistics change.)
    - In the folder for the account that you used to log in (for example, **C:\Inetpub\EFTRoot\GSSite\Usr\<username>**), you should see the files that you transferred.
5. If you are not able to connect, refer to Troubleshooting DMZ Gateway Communication.

Troubleshooting DMZ Gateway Communication

Various configurations can prevent the server and DMZ Gateway from communicating. For example, if the DMZ Gateway computer's firewall is blocking connections, the server will not be able to connect to DMZ Gateway.

If the status icon in DMZ Gateway does not change color to green indicating a successful connection, verify the following:

1. Verify that the services for the server and DMZ Gateway are started.
2. If you make changes in DMZ Gateway, make sure to click **Apply Changes**. If necessary, in the server, stop and then restart the service (and/or the Site in EFT) after making changes.
3. If you made configuration changes in EFT, especially connection settings (protocols allowed, ports, etc.), make sure to stop and then restart the EFT service. Once restarted, make sure EFT is running (listening for new connections) and that DMZ Gateway remains enabled.
4. Verify that the IP address for the server is not blocked in DMZ Gateway's **IP Access Exception** list. By default, all IP addresses are granted access until you block or allow specific addresses. (Refer to Controlling Access by IP Address for the procedure for blocking/unblocking IP addresses.)
5. Verify that the DMZ Gateway settings in the server have the proper IP address and port and that the allowed protocols and ports have been defined for allowed incoming client connections.
6. Try pinging from the server computer to the DMZ Gateway computer and from the DMZ Gateway computer to the server computer. If you cannot connect, verify that there is no firewall that would block connections.

If a connection between the server and DMZ Gateway is indicated, but clients cannot connect to the server through DMZ Gateway:

Verify that you can connect to the server using a client account from within your network.

If connection is successful, but clients cannot connect through DMZ Gateway, something is not configured properly in the DMZ Gateway settings, either in DMZ Gateway or in the server. Verify that the server and DMZ Gateway are connected (see above) and that, in the server <--> DMZ Gateway configuration settings, the correct protocols and ports are specified for incoming client connections to the Gateway. These are the ports on which external clients will connect to DMZ Gateway. If no protocol is enabled or the wrong port is defined, clients will not be able to connect.

If connection fails, there is a configuration issue in the server. Review your configuration of user accounts and connection settings.

Using DMZ Gateway as an Outbound Proxy

DMZ Gateway's primary use is as an inbound proxy. Outbound connections that originate from EFT will route through normal network mechanisms to reach the destination; however, it is possible to configure EFT's Event Rules using the **Copy/Move file to host** Action to use DMZ Gateway as an outbound proxy.

Viewing Statistics

In the DMZ Gateway administration interface, you can view a variety of statistics. Whether you click **All Profiles** or a specific Profile, the **Status**area displays information about Peer Notification Channels and Client Listeners, as well as the size and speed of server and client data being transferred.

Your selections persist across Profiles; that is, if you click the **Client Listeners** tab in Profile 3, then click Profile 2, the **Client Listeners**tab is selected in Profile 2 also.

The status "bubbles up" to the **All Profiles** node. For example, if there is a problem in Profile 1 causing the icon to turn yellow, the **All Profiles** icon is also yellow.

In the Profile tree:

- A red icon indicates that an error exists (e.g. port conflict from external application, IP address no longer exists, etc.).
- A yellow icon indicates that the DMZ Gateway service is running, but port conflicts exist between connected sites, when at least two Sites are connected.
- A green icon indicates that the DMZ Gateway Service is running and at least one Site is connected.
- A gray icon indicates that there are no errors and no Servers are connected.

Peer Notification Channels Tab

The **Peer Notification Channels**tab of the **Status** panel displays the IP address, port, number of active sites, channel status, and channel status message for each configured server-side IP address for a selected Profile or **All Profiles**. If **All Profiles** is selected, a Profile column displays the name of the applicable Profile. (For more about Peer Notification, refer to Introduction to Globalscape DMZ Gateway.)

The following icons provide an indication of channel status:

Active with connected servers

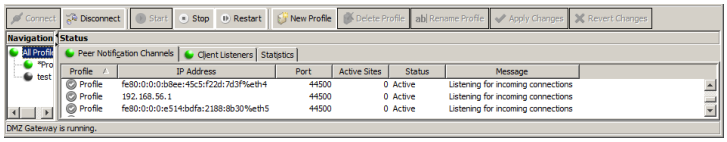
Active with no connected servers

Warning

Error

The following columns displayed on the tab can be sorted by clicking the column header:

- **IP address**- IP address on which Peer Notification Channels communicate
- **Port** - Port on which Peer Notification Channels communicates
- **Active Sites**- Number of Sites connected to DMZ Gateway
- **Status** - Active, Inactive, Warning, Error
- **Message** - More information regarding status (for example, Listening for connections, Port already in use)



Client Listeners Tab

The **Client Listeners** tab of the **Status** panel displays the PNC address, server IP address, server name, server type, Site name, listener IP address/port, status, and status message. If **All Profiles** is selected, the **Profile**column displays the name of the applicable Profile.

The following icons provide an indication of status:

- Listening
- Inactive
- Warning
- Error

The following columns displayed on the tab can be sorted by clicking the column header:

- **PNC Address**- Server-side IP address on which the server connected to DMZ Gateway
- **Server IP Address**- IP address of the remote server
- **Server Name**- user-assigned name of connected server
- **Server Type**- Type of server, e.g., EFT
- **Site** - User-assigned name of Site
- **Listener IP Address**- Client-side IP address on which clients connect to DMZ Gateway
- **Listener Port**- Port of Listener
- **Status** - Active, Inactive, Error, Warning

- **Message** - More information regarding status (for example, Listening for incoming connections, Unable to bind to port, Listener creation failure, Closed, Inactive, Listener IP/Port address already assigned)

Statistics Tab

The **Statistics** tab of the **Status** panel displays the size and speed of server and client data being transferred. When **All Profiles** is selected, the aggregated data sizes are displayed, and the **Profile** column displays the name of the applicable Profile.

The **Statistics** tab is configured by default to refresh automatically every 15 seconds. You can change the refresh frequency or configure the interface to not refresh automatically. You can also refresh the display manually.

- To change the refresh frequency, in the **Refresh Interval** box, provide a new interval, in seconds, then click **Apply Refresh Interval**.
- To prevent the interface from refreshing automatically, clear the **Enable automatic refresh**check box.
- To refresh the interface manually, click **Refresh Now**.

The following columns displayed on the tab can be sorted by clicking the column header:

- **Server IP Address**- IP address of the server
- **Client Bytes Read/sec**- Number of bytes received from Clients
- **Client Bytes Written/sec**- Number of bytes sent to Clients
- **Server Bytes Read/sec**- Number of bytes received from Servers
- **Server Bytes Written/sec**- Number of bytes sent to Servers
- **Accepted Client Connections**- Number of successful client connections.
- **Rejected Client Connections**- Number of client connections attempted that were rejected.

DMZ Gateway Secure PNC

The topics in this section describe how to enable and configure secure PNC in DMZ Gateway and EFT.

- Introduction to Secure PNC
- Remote Administration through DMZ Gateway
- Configuring Secure PNC
- Secure PNC Settings
- Secure PNC Logging

Introduction to Secure PNC

EFT administrators might want to administer EFT from a location external to the network by connecting through the DMZ Gateway instead of having to RDP in to the server. The Peer Notification Channel (PNC) between DMZ Gateway and EFT is not, itself, encrypted. Instead, the PNC leverages the encryption provided by the secure protocols (for example, FTPS, SFTP, HTTPS) in EFT. This inherently encrypts the traffic traversing through the DMZ Gateway and traffic will remain encrypted until it reaches EFT. In this way, the PNC is not susceptible to man-in-the-middle attacks and does not present any real world security risks as long as EFT is using secure protocols.

If you want to further enhance the security of the data passing through DMZ Gateway, you can enable secure PNC settings in DMZ Gateway and EFT. The secure PNC settings will reduce false positives for security scans and reduce the attack vector.

Configuring Secure PNC

Secure PNC will work using a self-signed certificate created with OpenSSL or one created from EFT. Depending on the certificate used, different configuration steps must be taken, as described below.

There are two ways of authenticating the communication between EFT and DMZ:

- Non-mutual authentication
  - EFT will blindly trust the DMZ Gateway certificate and DMZ Gateway will blindly trust the EFT certificate.
- Mutual authentication
  - EFT will only trust that single certificate and DMZ Gateway will require EFT to provide a client certificate during the SSL handshake and it must match the DMZ Gateway server's certificate trust store.

Configuring Secure PNC using a Self-Signed Certificate

To configure Secure PNC using a self-signed certificate

1. Stop the DMZ Gateway Service.
2. On the DMZ Gateway server, open a command prompt and navigate to **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin**.
3. Type the following command to create a self-signed certificate:

```
keytool -genkeypair -alias test -keyalg RSA -validity
        365 -keystore keystore.jks
```

4. Enter a keystore password (for example, test123!).
5. Follow the prompts for creating the self-signed certificate.
6. Follow the steps for Non-Mutual Authentication between EFT and DMZ or steps for Mutual Authentication between EFT and DMZ, above.

Configuring Secure PNC using an EFT Certificate

This certificate will be used later for Mutual Authentication with the DMZ Gateway server.

The procedure below requires OpenSSL to convert the public and private EFT keys into a .p12 format and Java's keytool to create a keystore.jks file.

***To* configure Secure PNC using an EFT-generated certificate**

1. Install EFT Server.
2. Launch the EFT administration interface.
3. Create the default Site with SSL enabled
4. Create a new SSL Certificate, making sure the certificate password is at least 6 characters long. (This certificate will not be associated with any EFT Site; this is used instead of creating a certificate using OpenSSL.)
5. Install OpenSSL (use version 1.0.2 or later).
6. Copy the private and public certificates from Step 4 into the bin directory of OpenSSL (this makes it easier), **C:\OpenSSL-Win32\bin**
7. Using OpenSSL, run the following (update where necessary):

   ```
   openssl pkcs12 -export -in [filename-certificate]
          -inkey [filename-key] -name [host] -out [filename-new-
   PKCS-12.p12]
   ```

   (Refer to https://www.wowza.com/docs/how-to-import-an-existing-ssl-certificate-and-private-keyfor information about how to convert the certificate and private key to PKCS 12 (.p12).)
8. If you see a warning related to "can't open config file," then cancel the entry from Step 7 and run this command instead:

   ```
   set OPENSSL_CONF=[path-to-OpenSSL-install-
   dir]\bin\openssl.cfg
          (i.e. set OPENSSL_CONF=c:\OpenSSL-Win32\bin\openssl.cfg)
   ```
9. When prompted for a passphrase, enter the certificate password you used when this certificate was created in EFT.
10. On the DMZ Gateway server, use Windows File Explorer to navigate to the DMZ Gateway installer's **/bin/**path, e.g., **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin**.
11. Copy the **.p12** certificate from Step 7 into the DMZ Gateway installer's **/bin/**path in the previous step. (This makes it easier to create the keystore.jks file.)
12. Open Command Prompt to the DMZ Gateway installer's **/bin/**path and enter the following command (update where appropriate):

    ```
    keytool -importkeystore -deststorepass [password]
    -destkeystore [filename-new-keystore.jks]
    -srckeystore [filename-new-PKCS-12.p12]
    -srcstoretype PKCS12
    ```

(where [password] is the original password set when the private key was created in Step 4)

You have successfully created a **keystore.jks**file that can be used to use non-mutual authentication between EFT and DMZ, described below.

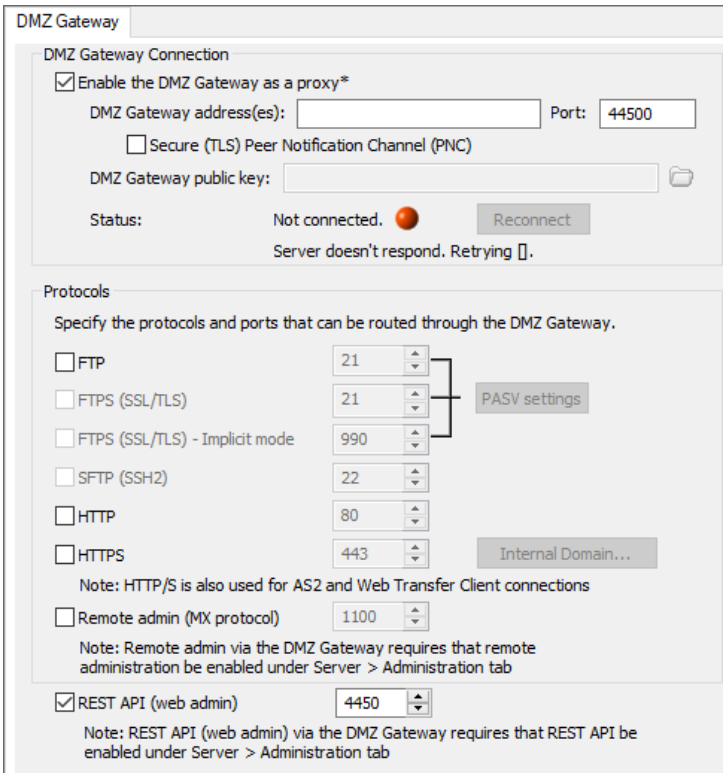
Non-Mutual Authentication setup

1. For simplicity, you can copy the **keystore.jks f**ile that was created above to a path that is easily accessible (for example, **C:\keystore\keystore.jks**), because you will have to paste the path in the DMZ Gateway xml configuration file.
2. Open Notepad or another text editor as an administrator.
3. Open the DMZ Gateway configuration file (gwconfig.xml), located in **C:\Program Files\GlobalSCAPE\DMZ Gateway.**

   (If the configuration file does not exist, start or restart the service and the file will be created.)
4. Set the <**SecurePNCEnabled**> value to "true."
5. Set the <**PNCKeyStorePath**> to the path where the **keystore.jks**is located (for example, **C:\keystore\keystore.jks**)

   > **NOTE:** You must enter the proper XML format for these values otherwise the service will not start, e.g., `<PNCKeyStorePath>c:\keystore\keystore.jks</PNCKeystorePath>`
6. Enter the store passphrase; because we imported the certificate into the keystore, this will default to the password created in EFT's certificate creation.
7. Save the XML file.
8. Close the XML file.
9. Start the DMZ Gateway service.
10. Re-open the XML file and verify the passphrase is now encrypted (this will also help confirm DMZ picked up the changes).

    NOTE If you are making any changes to the XML file, make sure the DMZ Gateway service has been stopped **prior to** making the changes.
11. To verify EFT detects that DMZ is configured, launch the EFT administration interface.



12. Click the **DMZ Gateway**tab.
13. Enable DMZ Gateway and provide the IP address of the DMZ Gateway, but do not select the **Secure TLS/PNC**check box.
14. Click **Apply**.
15. Verify that the EFT administration interface receives an error message.
16. Click **OK** on the error message.
17. Select the **Secure (TLS) Peer Notification Channel (PNC)** check box.
18. Click **Apply**.

DMZ Gateway and EFT are now configured with PNC SSL+ non-mutual authentication.

Mutual Authentication Setup

1. Copy the EFT SSL Site certificate (certificate associated with the SSL certificate settings) into the DMZ bin directory, e.g., **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin**.
2. Stop the DMZ Gateway Service.
3. To import EFT's SSL site certificate into the DMZ's Java truststore, open a command prompt and navigate to **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin**.
4. Run the following command:

```
keytool -import -alias EftClientCert -file "MySite
        Certificate.crt" -keystore truststore.jks
```

5. When prompted, enter the password of the keystore (not the password of the EFT site's certificate).
6. When prompted, type yes and press ENTER to trust the certificate.
7. Copy **truststore.jks**from the **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin** and place it in an easily accessible location (for example, **C:\keystore\truststore.jks**).
8. Open Notepad (or another text editor) as an administrator.
9. In Notepad, open the DMZ Gateway configuration (XML) file: **C:\Program Files\GlobalSCAPE\DMZ Gateway\gwconfig.xml**
10. Add the **PNCTrustStorePath**value, e.g., `<PNCTrustStorePath>c:\keystore\truststore.jks</PNCTrustStorePath>`.
11. Save and close the XML file.
12. To export the truststore certificate, open a command prompt and navigate to **C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin**.
13. Run the following command:

    ```
    keytool -export -alias test -keystore keystore.jks
            -rfc -file DMZGatewayCert.cer
    ```

14. If you don't recall the alias that you used, type the following command:

    ```
    keytool -list -v -keystore keystore.jks
    ```

    (This will give you the alias of your keystore)
15. When prompted enter the password of the keystore.
16. Copy the newly created certificate to EFT.
17. Log in to the EFT administration interface, and click the **DMZ Gateway** tab.
18. In the **DMZ Gateway public key**section, click the folder and navigate to the certificate that was copied to EFT.
19. Click **Apply**.

    Remote administration via the DMZ Gateway requires that remote administration be enabled on the **Server > administration** tab.

DMZ Gateway and EFT are now configured with Secure PNC with mutual authentication

Secure PNC Settings

After installing the DMZ Gateway, open **gwconfig.xml**in the root install folder with a text editor like Notepad. It should have the settings below for each DMZ Gateway profile.

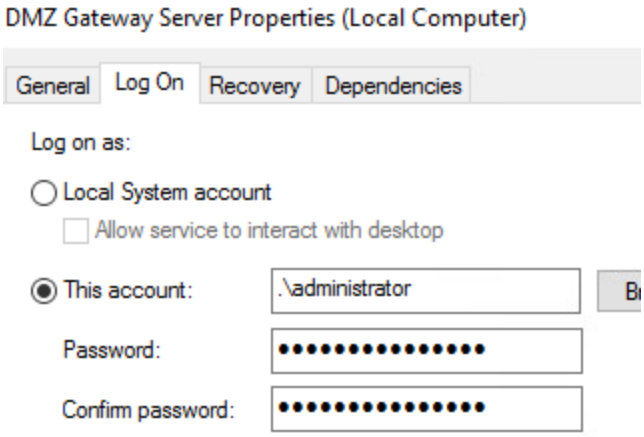
SecurePNCEnabled – This can be set to “true” or “false” to either enable or disable the secure PNC feature. By default this is false. If set to “true” you will also need to at a minimum provide values for the **PNCKeyStorePath**, **PNCStorePassphrase**, **PNCProtocols**, and **PNCCiphers**. If these aren’t set, the **DMZGatewayServer.log**file should contain log entries explaining what is missing.

If the **SecurePNCEnabled** setting is set to true, then it also acts like a “require SSL” setting in that only secure peer notification channels will be allowed. In other words, whether or not a channel is to be secured is enforced by the server and not solely dictated by the client.

PNCKeyStorePath – The full path to a Java keystore file which contains the certificate and private key (pair) that the DMZ Gateway will use for the PNC. By default, this has no value.

PNCKeyStore path supports network locations, however, the DMZ Gateway server service needs to have access to the network share. In this example, the network share on \\192.168.100.143 has the administrator account with access to it.

```
</NetworkAccessPolicy>
<AccelerationIP>AllIPv4</AccelerationIP>
<SecurePNCEnabled>true</SecurePNCEnabled>
<PNCKeyStorePath>\\192.168.100.143\keystore\keystore.jks</PNCKeyStorePath>
<PNCTrustStorePath>\\192.168.100.143\keystore\truststore.jks</PNCTrustStorePath>
<PNCTrustStorePath></PNCTrustStorePath>
<PNCStorePassphrase>OSBEjnEgz80U0x13GeqXroJ2DrQok8173iT19UhlUxGJqSvn508FOd3aVAqJio1EycJqYxy8gD2Ri57b42sa5f2Ytg==</PNCStorePassphrase>
<PNCProtocols>TLSv1.2,TLSv1.1</PNCProtocols>
<PNCCiphers>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECD
```



PNCTrustStorePath [Optional] – The full path to a Java keystore (that is, trust store) file which contains EFT’s certificate (just certificate, not private key) that is specified

on the EFT Site-level **Connections**tab in the **SSL Certificate Settings**dialog box. If a path is provided, client certificate authentication is required, and therefore EFT's certificate must exist in this keystore for the certificate to be trusted. If a path is not provided, then client certificate authentication is not required. By default, this has no value.

PNCStorePassphrase – This is that keystore passphrase for both the keystore and truststore mentioned above. You enter the password verbatim and then when the DMZ Gateway starts it will auto-encrypt the passphrase in the config file. By default, this has no value. PNCStorePassphrase is encoded to protect it from casual observance, but for added security it is recommended that you update the ACLs for the gwconfig.xml file to allow read and write access to only the account under which the DMZ Gateway service runs.

PNCProtocols – A comma separated list of protocols that the DMZ Gateway will allow for the secure PNC. This can take on the following values (by default set to TLSv1.2,TLSv1.1):

- TLSv1.2
- TLSv1.1
- TLSv1
- SSLv3 – This protocol is disabled by default by the JRE. To enable it you must update the java.security file under the install folder of the DMZ Gateway under "bin\jre1.8.0_74\lib\security" and remove SSLv3 from the line below:
- jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA…
- SSLv2Hello

PNCCiphers – Comma-separated list of cipher suites that the DMZ Gateway supports. Defaults to a list of secure ciphers that are supported by OpenJDK v17.0.2.

Per https://docs.oracle.com/javase/7/docs/technotes/guides/security/SunProviders.html#importlimits, Java, by default, limits the encryption strength (that is, maximum key size) for various algorithms due to import regulations in some countries. Therefore, to use stronger encryption like AES 256, you will need to deploy the JCE Unlimited Strength Jurisdiction Policy Files We aren't enabling that by default so that we can make sure we also comply with these import restrictions.

Also, the SSLEngine JCE API doesn't appear to support the cipher suite syntax such as "RSA+AES" or ! so the full cipher suite names must be specified.

Here is an example of the new config settings with sample values:

```
<SecurePNCEnabled>true</SecurePNCEnabled>
 <PNCKeyStorePath>C:\devel\certs\keystore.jks</PNCKeyStorePath>

<PNCTrustStorePath>C:\devel\certs\truststore.jks</PNCTrustStoreP
ath>

<PNCStorePassphrase>GSBEvsavuSo9cA6OO18fS5B+ubI+zdoDBYTzMoA3vtDQ
iiA65hLnVLdRAwyIZStqezbpLnbsu3E1IOH5Fh1Hij9qjQ==</PNCStorePassph
rase>
<PNCProtocols>TLSv1.2,TLSv1.1,TLSv1</PNCProtocols>
<PNCCiphers>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256</PNCCiphers>
```

List of cipher suites

In v4.0 of DMZ Gateway, the JDK/JRE update includes the following updated ciphers in gwconfig.xml:

```
"TLS_AES_128_GCM_SHA256",
"TLS_AES_256_GCM_SHA384",
"TLS_CHACHA20_POLY1305_SHA256",
"TLS_DHE_DSS_WITH_AES_128_CBC_SHA",
"TLS_DHE_DSS_WITH_AES_128_CBC_SHA256",
"TLS_DHE_DSS_WITH_AES_128_GCM_SHA256",
"TLS_DHE_DSS_WITH_AES_256_CBC_SHA",
"TLS_DHE_DSS_WITH_AES_256_CBC_SHA256",
"TLS_DHE_DSS_WITH_AES_256_GCM_SHA384",
"TLS_DHE_RSA_WITH_AES_128_CBC_SHA",
"TLS_DHE_RSA_WITH_AES_128_CBC_SHA256",
"TLS_DHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_DHE_RSA_WITH_AES_256_CBC_SHA",
"TLS_DHE_RSA_WITH_AES_256_CBC_SHA256",
"TLS_DHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA",
"TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
```

```
"TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA",
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
"TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA",
"TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA",
"TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384",
"TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDH_RSA_WITH_AES_128_CBC_SHA",
"TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDH_RSA_WITH_AES_256_CBC_SHA",
"TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384",
"TLS_EMPTY_RENEGOTIATION_INFO_SCSV",
"TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384",
"TLS_RSA_WITH_AES_128_CBC_SHA",
"TLS_RSA_WITH_AES_128_CBC_SHA256",
"TLS_RSA_WITH_AES_128_GCM_SHA256",
"TLS_RSA_WITH_AES_256_CBC_SHA",
"TLS_RSA_WITH_AES_256_CBC_SHA256",
"TLS_RSA_WITH_AES_256_GCM_SHA384"
```

Secure PNC Logging

In most cases, you can inspect the **DMZGatewayServer.log** for log entries of interest.

For more detailed SSL logging, edit the **DMZGatewayServerService.conf** file by uncommenting this line and restarting the DMZ Gateway server service:

```
#wrapper.java.additional.6=-Djavax.net.debug=ssl:handshake:data
```

This will print each SSL handshake message to the **DMZGatewayServerService.log** file.

Other options for javax.net.debug can be found in https://docs.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html#Debug.

It is generally easier to troubleshoot secure PNC communication issues from the perspective of the DMZ Gateway due to the detailed logging that Java offers through that **javax.net.debug** option.

You can also use Wireshark to observe the communication from another perspective and/or to validate that encryption is actually being used on the channel.

The EFT REST API

Refer to the topics below for more information about using the EFT REST API.

- Introduction to EFT's REST API
- Enabling REST API for Remote Administration
- Configuring REST Permission Roles
- Using REST API for Connection Profiles
- Using REST API to Retrieve Users Upload Quotas
- Using REST API to Retrieve Server and Site Metrics
- Authenticate REST-Authorized Administrators
- EFT REST API Reference (PDF)
- REST API Examples (ZIP download)

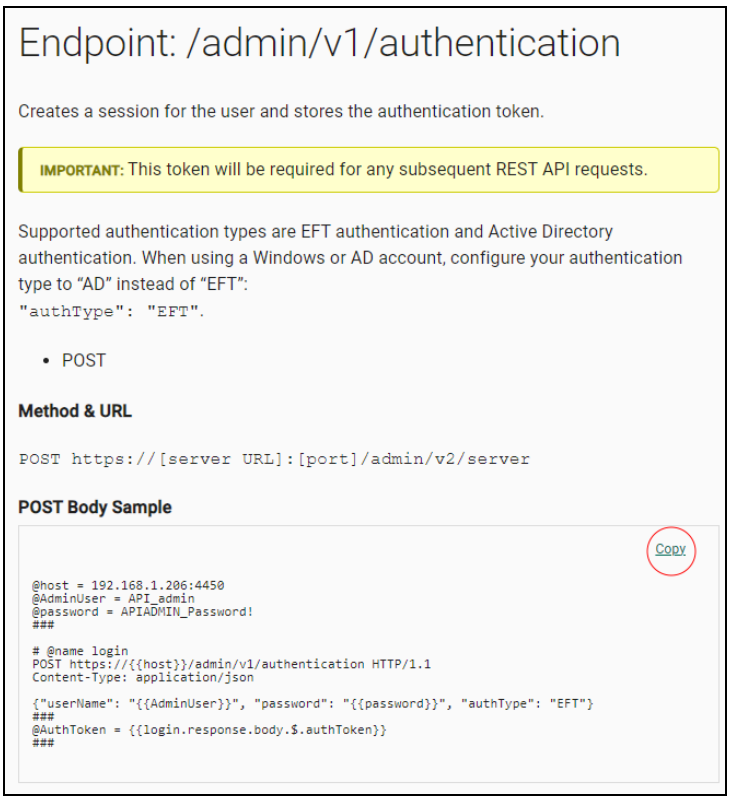
What is REST API?

REST (REpresentational State Transfer) API is an architectural style for an application program interface (API) that uses HTTP requests (GET, PUT, POST, DELETE) and a URI (resource identifier) to access and use data. There is no official standard for REST API however, the OpenAPI specification has become a common standard.

If you are new to REST APIs, here are a few tutorials that could help:

- freeCodeCamp
- Geeks for Geeks
- Medium.com

The endpoint references in this guide provide samples. In the HTML version of this guide, there is a Copy link next to each sample that copies the code to your computer's clipboard, making it available to paste into your scripts.



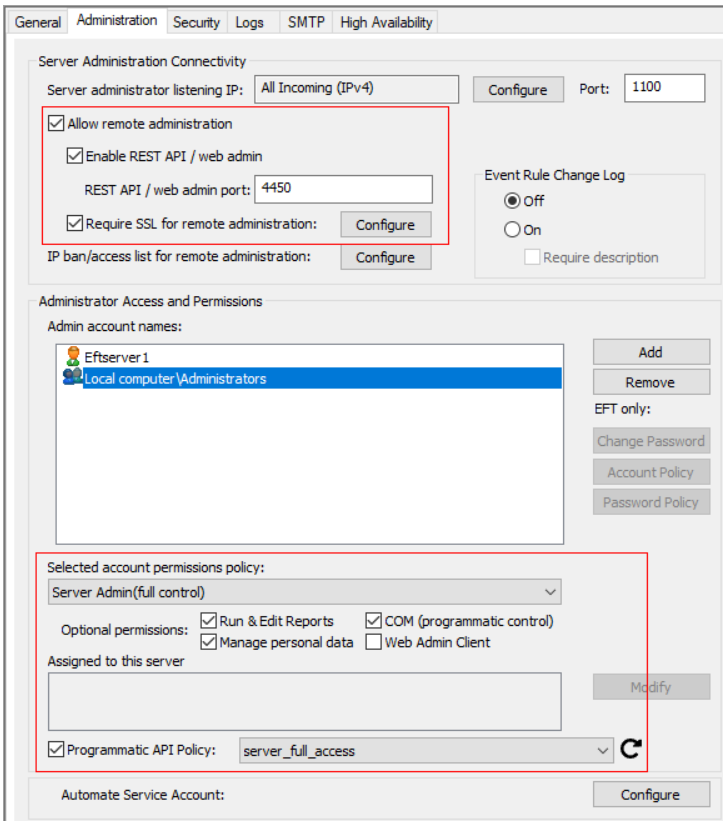
You can also download a ZIP file for examples.

Enabling REST API for Remote Administration

To use the EFT REST API to administer EFT remotely, you first must enable REST API in the EFT administration interface.

To enable REST API for remote administration

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server**tab, click the Server node that you want to manage.
3. In the right pane, click the **Administration**tab.



4. Select the **Allow remote administration** check box.
5. Select the **Enable REST API /web admin** check box.
6. Specify the **REST API /web admin port**. The default is 4450.
7. (Optional) Select the **Require SSL for remote administration** check box, then specify the SSL certificate to use.

8. At the bottom of the tab, select the **Programmatic API Policy**check box, and then select the **server_full_access** permission.

   > **NOTE:** When the **Web Admin Client** check box is selected, the Programmatic Policy automatically changes to "use account permission policy."

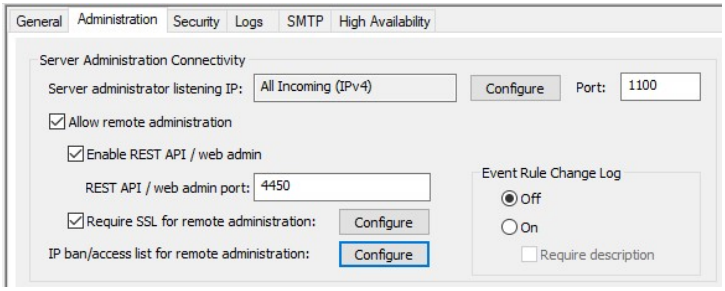
9. Click **Apply**to save the changes on EFT.

Refer to Configuring REST Permission Roles for details of the **Programmatic API Policy** settings and configuring REST permissions.

REST API Support via DMZ Gateway

EFT enables REST API support via DMZ Gateway so that you can maintain your current security posture. A Site admin or Server admin can add the REST API protocol to the DMZ Gateway. Whether added for one or more sites, the inbound connection to the specified IP:port will be routed to the REST API listener (a single, server-side listener).

REST API via the DMZ Gateway requires that the **REST API/ web admin** check box is selected on the EFT Server > **Administration** tab, under the **Allow remote administration** check box.



- You must have at least one whitelisted IP specified under IP Access Rules for Remote Administration.

Refer to Enabling REST API for Remote Administration for more information.

Configuring REST Permission Roles

REST permission roles are assigned to administrators by selecting an available role from the drop-down list to the right of the **REST administrator**role check box at the bottom of the **Site > Administration** tab. This list is populated by roles defined in **PermissionRoles.json** and are read every time the list control is clicked. Refer to Enabling REST API for Remote Admin for details of enabling the REST API.

> **NOTE:** When the **Web Admin Client** check box is selected, the Programmatic Policy automatically changes to "use account permission policy" and cannot be changed.

Server-level administrators can define a set of permissions for operations on one or more REST endpoints as a permissions role (aka policy) which can subsequently be assigned to one or more EFT administrators. These roles, not linked to existing administration access modes, allow precise control over what each administrator can and cannot do within the context of REST. Having roles defined in JSON gives server-level administrators maximum flexibility in the number, kinds, and granularity of permissions assigned to a role. The **PermissionRoles.json** file is created at installation (C:\ProgramData\Globalscape\EFT Server) with the default roles **server_read** and **server_full_access**, as shown below:

```
[
	{
	"name": "server_read",
	"enabled": true,
	"permissions": [
		"server:*:*:*:read",
		"sites:*:*:*:read"
		]
	},
	{
	"name": "server_full_access",
	"enabled": true,
	"permissions": [
		"server:*:*:*:*",
		"sites:*:*:*:*"
		]
	}
]
```

Each role composed of a name (maximum length 255 UTF-8 characters), a flag denoting whether the role is enabled, and a list of permissions strings. You can add additional permissions to the file as described below.

If you make changes to **PermissionRoles.json**, click the refresh icon to refresh the list on the Server > Administration tab. (This is also a good way to test that your changes to the JSON file are valid.)

Permissions String

The "permissions" string has five sections separated by colons (:). The sections, ordered from left to right, are Primary Area, Area, Sub Area, Item, and Action. For example, the sections of the permissions strings for the default "server_read" role above are:

Primary Area	Area	Sub Area	Item	Action
server:	*:	*:	*:	read
sites:	*:	*:	*:	read

The use of the wildcard '*' is explained below.

Primary Area, Area, Sub Area

Values for each section are:

Primary Areas	Areas	Sub Areas
server	server	settings
sites	sites	metrics
		settings
	users	settings
		personaldata
	eventrules	settings
	folders	settings
	ram	settings

Item:

Values that go in the Items section are names of name-value pairs used in JSON requests and responses. This provides permissions granularity down to the individual configuration setting level. Several items can be listed in this section with a comma between them.

Refer to Item listbelow.

Action:

- create
- read
- update
- delete
- execute

Several actions can be listed with commas between them. Not all actions are applicable to all items. Please refer to the endpoint documentation to know which actions are applicable to any given item.

An asterisk (*), meaning *all,* can be used for any section after the primary area. If an asterisk has been used for area or sub area an asterisk must be used for the item. If an item must be specific, that is no (*), then the area and sub area must also be specific. An exclamation mark (!) preceding a value means *all values except* the specified value. For example, this permission string allows an administrator to create users for any site and read all their settings but not delete the user or update their settings:

```
"sites[*]:users[*]:*:*:create,read"
```

Filters

Filters can be used with the sites primary area and all areas to target permissions to very specific cases and are defined by including an appropriate string inside brackets []. If (*) is used instead of a string it means *all*, or no filtering, and can be omitted if desired. So, if building a permissions string that applies to only one user, JaneDoe, for all sites you would use:

```
"sites[*]:users[JaneDoe]…"
```

Multiple filters can be specified by adding bracketed strings. A permissions string that applies only to two rules for all sites would look like:

```
"sites[*]:eventrules[MyFolderMonitor][MyTimer]…"
```

Matching filter strings to the area they are applied to is the default. That is, the default filter behavior for the users area is to apply the filter string against user names, for the folders area is to apply the filter string against folder names, etc. Filters can be applied to special filter areas other than their default area. The special filter areas are:

- usergroup
- usertemplate
- eventrulefolder
- eventrules
- node

To apply a filter to one of these special filter areas the area must prefix the filter string with a colon (:) separating them. For instance, a permissions string that applies only to users belonging to the Guest user group on the site MySite would start this way:

```
"sites[MySite]:users[usergroup:Guest]:……"
```

In addition to using filters to single out a few special cases in which to apply the permission string, they can also be used to exclude special cases. By prefixing the string with "*,!" exceptions can be specified. So, a permissions string that is intended to apply to every user on a site except for JohnDoe would begin like this:

```
"sites[MySite]:users[*,!JohnDoe]:……"
```

Examples

Below are examples of permissions strings categorized by general use case:

User-Related Permissions:

Admin can create users and configure everything about those users:

```
"sites[*]:users[*]:*:*:create,read,update"
```

Admin can create users except for a user name matching "Administrator":

```
"sites[*]:users[*,!Administrator]:*:*:create"
```

Admin can read all the configuration for all users for a given site named "MeeTooSite":

```
"sites[MeeTooSite]:users[*]:*:*:read"
```

Admin can read the AllowSecureFolderSharing value for users in the Guest Users template, but cannot read any other values or do anything else:

```
"sites[*]:users[settingstemplate:Guest
Users]:settings:AllowSecureFolderSharing:read"
```

Note: When an admin with only this users permission does a GET on users, the response will contain only the users belonging to the Guest Users template. If the admin does a get on a user belonging to Guest Users, only the UUID and the value for AllowSecureFolderSharing is returned. Since name isn't allowed per this permission then name will not be returned.

Admin can read the configuration to find out everything about all users in Site "MySite" under template "Guest Users" but not make any changes to those users:

```
"sites[MySite]:users[settingstemplate:Guest
Users]:*:*:read"
```

Admin can update everything about any user:

```
"sites[*]:users[*]:*:*:update"
```

Admin can update everything about any user except for changing their SFTP key:

```
"sites[*]:users[*]:connection:*,!sftpkey:update"
```

Admin can update all users except for a user matching a specific name of "John":

```
"sites[*]:users[*,!John]:*:*:read,update"
```

Admin can update users but not create them or delete them:

```
"sites[*]:users[*]:*:*:read,update"
```

Admin can delete users:

```
"sites[*]:users[*]:*:*:delete"
```

Admin can delete all users except for a user named "John":

```
"sites[*]:users[*,!John]:*:*:delete"
```

VFS-Related Permissions:

Admin can read and create maps for the folder "bin":

```
"site[MySite]:folders[/bin/]:folders:maps:create,read"
```

Admin can create, update, and read folder names for the "usr" folder:

```
     "site[MySite]:folders
[/usr/]:folders:folder:create,read,update"
```

Admin can read and update permissions for the folder "bin":

```
     "site[MySite]:folders
[/bin/]:folders:permissions:read,update"
```

Admin can read and change the encrypt setting for folders in the folder "bin":

```
     "site[MySite]:folders [/bin/]:folders:encrypt:read,update"
```

Item list

server:server:metrics:	activeclientdownloadbytespersecond activeclientdownloadcount activeclientuploadbytespersecond activeclientuploadcount activeserverdownloadbytespersecond activeserverdownloadcount activeserveruploadbytespersecond activeserveruploadcount connectedadmincount connectedusercount runningawtaskcount runningeventrulecount isnodemaster isnodestarted licensemodules localtime nodename uptime

server:server:settings:	ha.enabled
	smtp
	smtp.login
	smtp.password
	smtp.port
	smtp.senderaddr
	smtp.sendername
	smtp.server
	smtp.useauthentication
	smtp.useimplicittls
	general.configfilepath
	general.lastmodifiedby
	general.lastmodifiedtime
	general.useutcinlistings
	listenersettings.adminport
	listenersettings.allowremoteadministration
	listenersettings.listenips
	listenersettings.localips
	logs.audit
	logs.audit
	logs.audit
	logs.audit
	logs.audit
	logs.audit

	logs.logfilepath logs.audit.password logs.audit.connected version nodename

sites[ ]:sites:settings	dmz.enabled dmz.server.ipaddresses dmz.server.nodename dmz.server.port general.authtype general.disabledusercount general.lastmodifiedby general.lastmodifiedtime general.rootfolder general.usercount listenersettings listenersettings.httpdomain listenersettings.accountmanagementurl listenersettings.listenips listenersettings.ftpsimplicitport listenersettings.ftpport listenersettings.ftpsport listenersettings.httpsport listenersettings.httpport listenersettings.sftpport name workspacessettings.enabled

sites[ ] :sites:metrics:	definedusers isdmzgatewayconnected isrunning name activeclientdownloadbytespersecond activeclientdownloadcount activeclientuploadbytespersecond activeclientuploadcount activeserverdownloadbytespersecond activeserverdownloadcount activeserveruploadbytespersecond activeserveruploadcount connectedusercount node.name runningawtaskcount runningeventrulecount starttime state dmzconnected

sites[ ]:users:connections:	as2.inbound.enabled as2.outbound.enabled ftp.enabled ftp.value.banner.message ftp.value.banner.usage ftp.value.enablecomb ftp.value.enablefxp ftp.value.enablenoop ftp.value.enablexcrc ftp.value.enablezlib ftps.enabled http.enablehttp http.enablehttps http.enablesendmessage http.enablesharefolder http.enablewtc sftp.enabled sftp.value.authenticationtype ssl.authenticationtype transferspeedlimit.enabled transferspeedlimit.value.maxkbps uploadsizelimit.enabled uploadsizelimit.value.maxkbytes uploadspersessionlimit.enabled

	uploadspersessionlimit.value.maxnumber downloadsizelimit.enabled downloadsizelimit.value.maxkbytes downloadspersessionlimit.enabled downloadspersessionlimit.value.maxnumber connectiontimeout.enabled connectiontimeout.value.maxsec connectionsfromsameiplimit.enabled connectionsfromsameiplimit.value.maxnumber totalconnectionslimit.enabled totalconnectionslimit.value.maxnumber sshkeys.data sslcertificate.data

sites[ ]:users:settings:	accountenabled agreementtotermsofservice changepassword.enabled changepassword.value.changeadminprovidedpasswordduponfirstuse changepassword.value.mustchangepassword changepassword.value.passwordexpiration.enabled changepassword.value.passwordexpiration.emailupon changepassword.value.passwordexpiration.maxagedays changepassword.value.passwordexpiration.remindprior consenttoprivacypolicy expiration.enabled expiration.value.date externalauthentication hashomefolderasroot homefolder.enabled homefolder.value.path inactivitylimit.enabled inactivitylimit.value.action inactivitylimit.value.days invalidloginlimit.enabled invalidloginlimit.value.action invalidloginlimit.value.actiondurationmin invalidloginlimit.value.maxcount invalidloginlimit.value.periodmin

	iseudatasubject loginname passwordcomplexity.enabled passwordcomplexity passwordhistory.enabled passwordhistory.value.historydepth ipaccesslimit.enabled ipaccesslimit.value.defaultrule ipaccesslimit.value.rules settingstemplate.data permissiongroups.data

sites[ ]:users:personaldata	personal.duns personal.comments personal.company personal.custom1 personal.custom2 personal.custom3 personal.description personal.email personal.fax personal.mobile personal.name personal.pager personal.partnerid personal.phone

sites[ ]:users:as2in:	mdnsendattemptdelayseconds mdnsendattemptretries mdnsendattempttimeoutseconds micalgorithm allowedencryptionalgorithms allowedsignaturealgorithms authenticationtype contentcollision donotsend100continue foldertomovedatato myid partnercertificatefilepath partnerid rejectidmismatch rejectmessageidcollision rejectnotencrypted rejectnotsigned rejectpartneridmismatch renamefilesto transactionfailedcommandsettings transactionfailedcommandsettings.parameters transactionfailedcommandsettings.workingdirectory transactionfailedemail.bcc transactionfailedemail.body

	transactionfailedemail.cc transactionfailedemail.ccuser transactionfailedemail.from transactionfailedemail.subject transactionfailedemail.to transactionsuccesscommandsettings transactionsuccesscommandsettings.parameters transactionsuccesscommandsettings.workingdirectory transactionsuccessemail transactionsuccessemail.bcc transactionsuccessemail.body transactionsuccessemail.cc transactionsuccessemail.ccuser transactionsuccessemail.from transactionsuccessemail.subject transactionsuccessemail.to transactionfailedcommand.data transactionsuccesscommand.data

sites[ ]:users:as2out:	asyncmdntimeoutminutes compress contenttype deletefileafteroffload encrypt encryptionalgorithm fileexclude fileinclude headers hotfolderpath myid partnercertificatefilepath partnerid proxy.enable proxy.value proxy.value.httpproxy.host proxy.value.httpproxy.port proxy.value.httpproxy.username receipt receiptdelivery sendattemptdelayseconds sendattemptretries sendattempttimeoutseconds serverhost

	serverpath serverport serverusername sign signaturealgorithm subject transactionfailedcommandsettings.parameters transactionfailedcommandsettings.workingdirectory transactionfailedemail.bcc transactionfailedemail.body transactionfailedemail.cc transactionfailedemail.ccuser transactionfailedemail.from transactionfailedemail.subject transactionfailedemail.to transactionsuccesscommandsettings.parameters transactionsuccesscommandsettings.workingdirectory transactionsuccessemail.bcc transactionsuccessemail.body transactionsuccessemail.cc transactionsuccessemail.ccuser transactionsuccessemail.from transactionsuccessemail.subject transactionsuccessemail.to

	transactionfailedcommand.data transactionsuccesscommand.data
sites[ ]:folders:settings:	name target
sites[ ]:eventrules:settings:	info.description info.enabled info.folder info.name info.next info.remote info.type info statements trigger folder

Using REST API for Connection Profiles

The example below can be used to get a list of connection profiles.

```
################################################

##############  Connection Profiles  ##############

### GET a list of current connection profiles###

# @name CP_List

GET https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###

@ConnectionProfileID = {{CP_List.response.body.$.data[0].id}}

### GET Details for specific connection profile####

GET https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles/
{{ConnectionProfileID}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

### DELETE specific connection profile####

DELETE  https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles/
{{ConnectionProfileID}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

### Create a Connection Profile ###

POST https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles/ HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

{

"data": {

"attributes": {

"name": "APIaa1_POST_Test_13",

"description": "POST REQUEST FAILS TO ADD USER DETAILS",

"testPath": "c:\\test",

"connectionSettings": {

"protocol": "FTPSAuthTLS",

"host": "192.168.1.210",

"port": 21,

"user": "AFAR",

"password": "",

"autoLogin": true,

"proxySettings": {
```

```
"use": true,
"type": "FTP",
"hostName": "123",
"username": "123",
"password": "UpKUJq1sD4Yfb1Hz8ZFiRw==",
"port": 21,
"subType": 0,
"separator": "@",
"customCommands": []
},
"SOCKSSettings": {
"use": true,
"type": "None",
"hostName": "123",
"port": 1080,
"auth": false,
"username": "123",
"password": "555"
},
"advancedSettings": {
"numberOfConnectionRetries": 11,
"delayBetweenRetries": 22,
"maxConcurrentThreads": 4,
"connectionTimeout": 55,
"dataPortMode": "AUTO",
"PASVPortMin": 5,
"PASVPortMax": 50000,
"preserveLocalTimeStamp": true,
"preserveRemoteTimeStamp": true,
"validateFileIntegrity": true,
"homeIP": "192.168.1.*",
"clearCommandChannel": true,
"clearDataChannel": true,
"transferEncoding": "UTF8"
}
}
}
```

```
}
}
####
```

Using REST API for Upload Quotas

The example below can be used to get and set upload quotas for specific users. As usual, you will need to change the user name, user folder, and so on.

```
###############################################################################
###This Request GETS the "Upload Quota at USR folder level"
###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
###############################################################################
#####    #########
##### GET the Folder structure and settings for a specifc User   #########
@User_Folder = AFAR
GET https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/
%2Fusr%2F{{User_Folder}}%2F HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###############################################################################
##### or ENTER THE USER NAME DIRECTLY ON THE CALL  #########
GET https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/
%2Fusr%2Ftony%2F HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###############################################################################
##### POST REQUEST TO CREATE A FOLDER WITH UPLOAD QUOTA ENABLED #########
###
@User_Folder = sofia
POST https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/
%2Fusr%2F{{User_Folder}}%2F/folders HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
"data": {
"type": "folder",
"attributes": {
"name": "Folder4",
"subFolder": "Folder4",
```

```
"uploadQuota": {
"emailsToReportToOnExceed": [
"gsqaaf1@gmail.com",
"gsqaaf2@gmail.com"
],
"enabled": true,
"limitMBytes": 150,
"usedMBytes": 0
}
}
}
}
###############################################################################################
##### UPDATE SETTINGS OF A SPECIFIC FOLDER FOR A SPECIFIC USER  #########
@User_Folder = sofia
@FOLDER_NAME = FOLDER4
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/
%2Fusr%2F{{User_Folder}}%2F{{FOLDER_NAME}}%2f HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
"data": {
"attributes":{
"uploadQuota": {
"emailsToReportToOnExceed": [
"gsqaaf1@gmail.com",
"gsqaaf2@gmail.com"
],
"enabled": true,
"limitMBytes": 150,
"usedMBytes": 0
}
}
}
}
###############################################################################
############ DELETE A SPECIFIC FOLDER FOR A SPECIFIC USER  ######################
@User_Folder = sofia
```

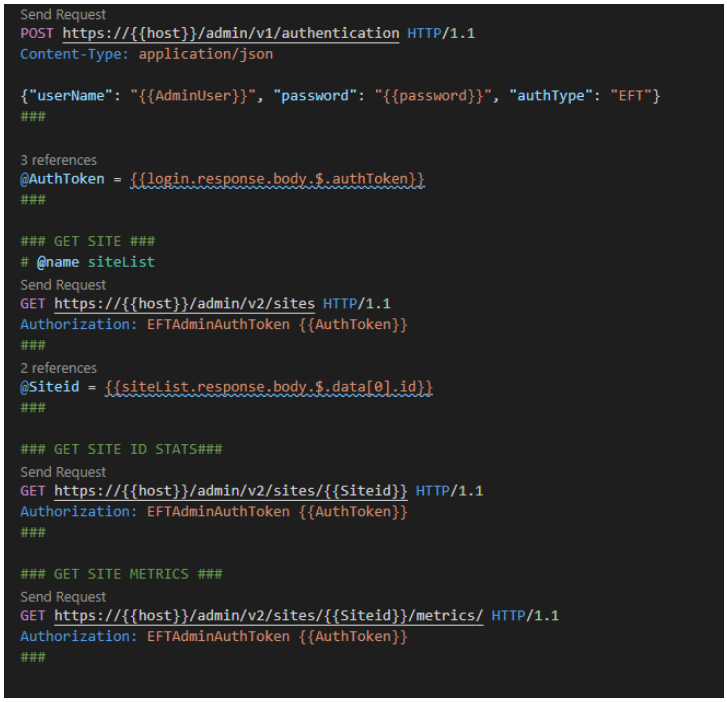
```
@FOLDER_NAME = FOLDER4
###
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/
%2Fusr%2F{{User_Folder}}%2F{{FOLDER_NAME}}%2f HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

Using REST API to Retrieve Server and Site Metrics

Using REST API calls, after authenticating with the Server, you an retrieve the Server statistics and metrics, Site statistics and metrics, and Node statistics and metrics.

The screenshots below show the entries used to make the REST calls.

```
# @name login
Send Request
POST https://{{host}}/admin/v1/authentication HTTP/1.1
Content-Type: application/json

{"userName": "{{AdminUser}}", "password": "{{password}}", "authType": "EFT"}
###

2 references
@AuthToken = {{login.response.body.$.authToken}}
###

### GET SERVER STATS###
Send Request
GET https://{{host}}/admin/v2/server HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###

### GET SERVER METRICS ###
Send Request
GET https://{{host}}/admin/v2/server/metrics/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```



```
Send Request
POST https://{{host}}/admin/v1/authentication HTTP/1.1
Content-Type: application/json

{"userName": "{{AdminUser}}", "password": "{{password}}", "authType": "EFT"}
###

3 references
@AuthToken = {{login.response.body.$.authToken}}
###

### GET SITE ###
# @name siteList
Send Request
GET https://{{host}}/admin/v2/sites HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
2 references
@Siteid = {{siteList.response.body.$.data[0].id}}
###

### GET SITE ID STATS###
Send Request
GET https://{{host}}/admin/v2/sites/{{Siteid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###

### GET SITE METRICS ###
Send Request
GET https://{{host}}/admin/v2/sites/{{Siteid}}/metrics/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

```
3 references
@host = 192.168.100.142:4450
1 reference
@AdminUser = admin
1 reference
@password = [redacted]
###

# @name login
Send Request
POST https://{{host}}/admin/v1/authentication HTTP/1.1
Content-Type: application/json

{"userName": "{{AdminUser}}", "password": "{{password}}", "authType": "EFT"}
###

2 references
@AuthToken = {{login.response.body.$.authToken}}
###

### GET NODE ###
# @name nodeList
Send Request
GET https://{{host}}/admin/v2/nodes HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
1 reference
@nodeID = {{nodeList.response.body.$.data[0].id}}
###

### GET NODE METRICS###
Send Request
GET https://{{host}}/admin/v2/nodes/{{nodeID}}/metrics/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

Using REST API to Authenticate REST-Authorized Administrators

There are multiple ways to use REST API and many tools. One helpful tool is Visual Studio Code (free tool) with the add-in for REST API.

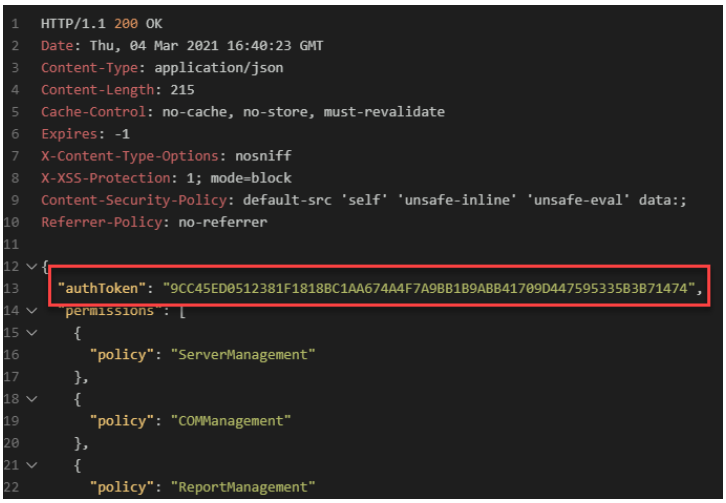
Make sure that REST API is enabled, as well as SSL for remote administration.

Here is an example of the REST API call that needs to be called to first authenticate with the EFT administrator user that has permission. Then you can make subsequent calls to EFT to allow access to the REST API endpoints:

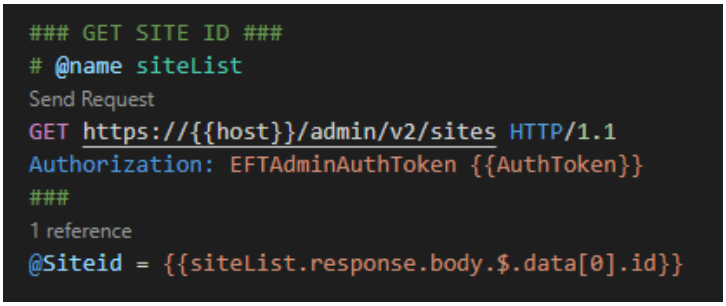
```
@host = 192.168.100.144:4450
1 reference
@AdminUser = admin
1 reference
@password = AdminPassword
###

# @name login
Send Request
POST https://{{host}}/admin/v1/authentication HTTP/1.1
Content-Type: application/json

{"userName": "{{AdminUser}}", "password": "{{password}}", "authType": "EFT"}
###

2 references
@AuthToken = {{login.response.body.$.authToken}}
###

### GET SITE ID ###
# @name siteList
Send Request
GET https://{{host}}/admin/v2/sites HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

You have defined your host (EFT Server), administrator (user and password), and then a POST request is sent to get the AuthToken. This is system generated as a response, which is then stored into a variable to pass on to subsequent requests.

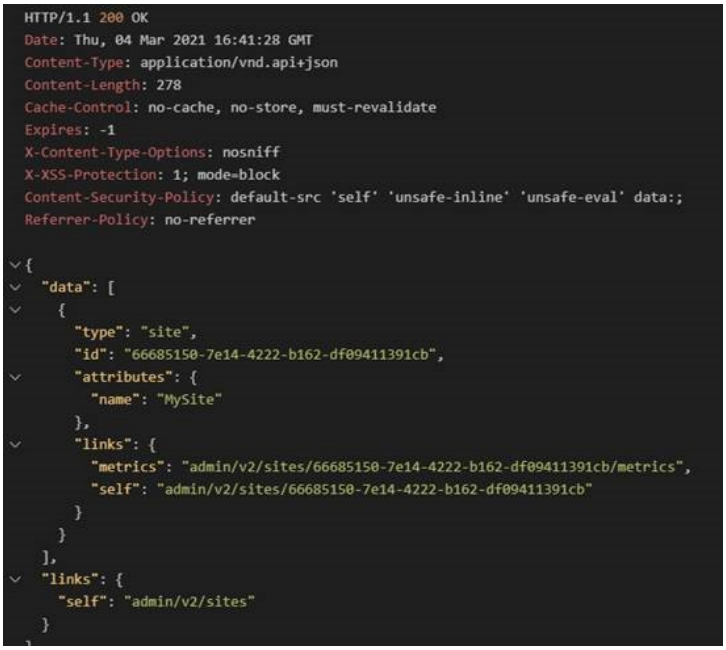
When you make a post request, EFT will respond with an authToken:



And then subsequent requests can be called using the same AuthToken:



Response from EFT:



As previously mentioned there are multiple tools that end-users can use to execute REST API calls, but Visual Studio Code is a great tool for end-users getting familiar with REST API functionality.

The JSON file to create permissions or modify REST API permissions is found in the EFT installation files here: \ProgramData\Globalscape\EFT Server\PermissionRoles.Json.

Server REST API

The endpoints described in this section are related to the server.

- Endpoint: /server
- Endpoint:/server/status
- Endpoint: /server/metrics
- Endpoint: /server/security/tls
- Endpoint: /server/security/ssh
- Endpoint: /server/reports
- Endpoint: /server/admin-users
- Endpoint: /server/admin-users/{adminId}
- Endpoint: /server/admin-users-policy
- Endpoint: /experimental/server/templates/{templateName}
- Endpoint:/server/ha/upgrade

Endpoint: /server

Returns and update server settings.

- GET
- PATCH

Method & URL

`GET https://[server URL]:[port]/admin/v2/server`

GET Body Sample

```
GET https://{{host}}/admin/v2/server HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}
```

GET Response Body Sample

```
{
"data": {
"type": "server",
"id": "1",
"attributes": {
  "version": "8.0.6.16",
  "general": {
     "configFilePath": "C:\\ProgramData\\Globalscape\\EFT Server Enterprise\\",
     "enableUtcInListings": true,
      "lastModifiedBy": "admin",
      "lastModifiedTime": 1633717057
     },
     "listenerSettings": {
        "adminPort": 1100,
        "enableRemoteAdministration": true,
         "listenIps": [ "0.0.0.0" ],
…
}
```

GET PowerShell Sample

```
#get Server
Write-Output "Get Server"
Write-Output "-----"
$serverDetails = Invoke-RestMethod -Uri "$baseURL/v2/server" -Method 'GET' -Headers
$authHeader
Write-Output $serverDetails | ConvertTo-Json
foreach ($server in $serverDetails.data)
{
    Write-Output ("Server $($serverDetails.data)")
}
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/server
```

PATCH Body Sample

```
PATCH  https://{{host}}/admin/v2/server HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
"data": {
    "type": "server",
    "id": "1",
    "attributes":{
        "version":"",
    "smtp": {
        "login": "",
        "password": "",
        "port": 587,
        "senderAddr": "EFT@mailserver.net",
        "senderName": "Globalscape EFT",
        "server": "smtp.mailserver.net",
        "useAuthentication": false,
        "useImplicitTLS": false
      }
    }
```

```
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

PATCH PowerShell Sample

```
##Patch Server - patching the SMTP settings
Write-Output "Server Patch"
Write-Output "-----"
$update =
'{
    "data":{
        "type": "server",
        "id": "1",
        "attributes": {
            "version": "",
        "smtp": {
            "login": "",
            "password": "",
            "port": 587,
            "senderAddr": "EFT@mailserver.net",
            "senderName": "Globalscape EFT",
            "server": "smtp.mailserver.net",
            "useAuthentication": false,
            "useImplicitTLS": false
         }
         }
     }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/server" -Method 'PATCH' -Headers
$authHeader -Body $update
```

Endpoint:/server/status

Returns server information

> **NOTE:** This endpoint works in v8.1, but not in v8.2 and later

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v1/server/status
```

GET Body Sample

```
GET https://{{host}}/admin/v1/server/status HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{"nodes":[{"activity":
{"activeClientDownloadBytesPerSecond":0,"activeClientDownloadCount":0,
"activeClientUploadBytesPerSecond":0,"activeClientUploadCount":0,"activeServerDownloadBytesPerSecond":0,
"activeServerDownloadCount":0,"activeServerUploadBytesPerSecond":0,"activeServerUploadCount":0,
"connectedAdminCount":1,"connectedUserCount":0,"runningAwTaskCount":0,"runningEventRuleCount":0},
"isInCluster":false,"isMaster":false,"isStarted":true,"licenses":[{"module":"AAMModule",
"registrationState":"Evaluation period"},
{"module":"ARMModule","registrationState":"Evaluation period"},
{"module":"AS2Module","registrationState":"Evaluation period"},{"module":"AWModule",
"registrationState":"Evaluation period"},{"module":"AccelerateModule",
"registrationState":"Requires Activation"},{"module":"CloudConnectorModule",
"registrationState":"Evaluation period"},
{"module":"DMZGWModule","registrationState":"Evaluation period"},
{"module":"EFTServer","registrationState":"Evaluation period"},
{"module":"EnterpriseActionsWModule",
"registrationState":"Evaluation period"},
{"module":"FTPModule","registrationState":"Evaluation period"},
{"module":"FileTransferClientModule","registrationState":"Evaluation period"},
{"module":"FolderMonitorEventModule",
```

```
"registrationState":"Evaluation period"},
{"module":"HSModule","registrationState":"Evaluation period"},

{"module":"HTTPModule","registrationState":"Evaluation period"},{"module":"PGPModule",

"registrationState":"Evaluation period"},
{"module":"RAModule","registrationState":"Evaluation period"},

{"module":"SSHModule","registrationState":"Evaluation period"},
{"module":"SecureFormsModule",

"registrationState":"Evaluation period"},
{"module":"TimerEventModule","registrationState":"Evaluation period"},

{"licensesAvailable":100,"module":"WorkspacesModule","registrationState":"Evaluation
period","usedLicenses":0}],

"localTime":1659595722,"name":"DY-Win2019-1a","upTime":52215}]}
```


GET PowerShell Sample

```
#get Server Metrics

Write-Output "Get Server Metrics"

Write-Output "-----"

$serverMetrics = Invoke-RestMethod -Uri "$baseURL/v1/server/status"

-Method 'GET' -Headers $authHeader

Write-Output $serverMetrics | ConvertTo-Json

foreach ($server in $serverMetrics.data)

{

    Write-Output ("Server $($serverMetrics.data)")

}
```

Endpoint: /server/metrics

Returns server metrics.

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/server/metrics
```

GET Body Sample

```
GET https://{{host}}/admin/v2/server/metrics HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{"data": {
"type": "serverMetrics",
   "id": "1",
"attributes": {
"activeClientDownloadBytesPerSecond": 0,
"activeClientDownloadCount": 0,
"activeClientUploadBytesPerSecond": 0,
"activeClientUploadCount": 0,
"activeServerDownloadBytesPerSecond": 0,
"activeServerDownloadCount": 0,
"activeServerUploadBytesPerSecond": 0,
"activeServerUploadCount": 0,
"connectedAdminCount": 1,
"connectedUserCount": 0,
"runningAwTaskCount": 0,
"runningEventRuleCount": 0
}

},
"links": {
      "self": "admin/v2/server/metrics"  }
```

```
}
```

GET PowerShell Sample

```
#get Server Metrics

Write-Output "Get Server Metrics"

Write-Output "-----"

$serverMetrics = Invoke-RestMethod -Uri "$baseURL/v2/server/metrics" -Method 'GET' -
Headers $authHeader

Write-Output $serverMetrics | ConvertTo-Json

foreach ($server in $serverMetrics.data)

{

    Write-Output ("Server $($serverMetrics.data)")

}
```

Endpoint: /server/security/tls

Returns and updates server TLS security settings.

- Get
- PATCH

Method & URL

`GET https://[server URL]:[port]/admin/v2/server/security/tls`

GET Body Sample

```
GET https://{{host}}/admin/v2/server/security/tls HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
"data": {
"type": "tlsServerSecuritySettings",
"id": "1",
"attributes": {
"tlsSettings": {
"minimumProtocolVersion": "TLSv1.3",
"selectedAlgorithms":
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:
EECDH+CHACHA20:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3DES:
RSA+3DES:EECDH+RC4:RSA+RC4:!MD5:!SRP:!PSK:!EXP:!RC4:!SSLv3:!SHA1",
"resultingCipherList":
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:
ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-CCM8:ECDHE-ECDSA-AES128-CCM:
ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:AES128-CCM8:
AES128-CCM:AES128-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:
ECDHE-ECDSA-AES256-CCM8:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA384:AES256-GCM-SHA384:AES256-CCM8:AES256-CCM:AES256-SHA256",
```

```
"manuallySelectedAlgorithms": {
"enabled": false,
"algorithms":
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_
SHA256:EECDH+CHACHA20:
EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3DES:RSA+3DES:EECDH+RC4:RSA+RC4:!M
D5:
!SRP:!PSK:!EXP:!RC4:!SSLv3:!SHA1"
}
},
"tlsFipsEnabled": false
}},
"links": {
"self": "admin/v2/server/security/tls"
}
}
```

GET PowerShell Sample

```
#get Server TLS Security Settings
Write-Output "Get Server TLS Settings"
Write-Output "-----"
$serverTLS = Invoke-RestMethod -Uri "$baseURL/v2/server/security/tls" -Method
'GET' -Headers $authHeader
Write-Output $serverTLS | ConvertTo-Json
foreach ($server in $serverTLS.data)
{
Write-Output ("Server $($serverTLS.data)")
}
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/server/security/tls
```

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/server/security/tls HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

```
{
"data": {
"type": "tlsServerSecuritySettings",
"id": "1",
"attributes": {
"tlsFipsEnabled": true
}
},
"links": {
"self": "admin/v2/server/security/tls"
}
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

PATCH PowerShell Sample

```
###(PATCH) TLS Security Settings (enable FIPS)
Write-Output "Server TLS Enable FIPS Patch"
Write-Output "-----"
$update =
'{
 "data": {
    "type": "tlsServerSecuritySettings",
    "id": "1",
    "attributes": {
      "tlsFipsEnabled": true
    }
  },
  "links": {
    "self": "admin/v2/server/security/tls"
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
```

```
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/server/security/tls" -Method 'PATCH'
-Headers $authHeader -Body $update
```

Endpoint: /server/security/ssh

Returns and update server SSH security settings.

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/server/security/ssh
```

GET Body Sample

```
GET https://{{host}}/admin/v2/server/security/ssh HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
"data": {
"type": "sshServerSecurity",
"id": "1",
"attributes": {
"sshSettings": {
"allowedCiphersList": "aes256-gcm@openssh.com,aes256-ctr,aes256-cbc,rijndael-
cbc@lysator.liu.se,
aes192-ctr,aes192-cbc,aes128-gcm@openssh.com,aes128-ctr,aes128-cbc",
"allowedKexesCiphersList": "ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,
diffie-hellman-group16-sha512,diffie-hellman-group14-sha256,diffie-hellman-group-
exchange-sha256",
"allowedMacsList": "hmac-sha2-512-etm@openssh.com,hmac-sha2-512,hmac-sha2-256-
etm@openssh.com,
hmac-sha2-256,hmac-sha1-etm@openssh.com,hmac-sha1",
"softwareVersion": "8.1.0.0_openssh",
"comments": "Globalscape"    },
"sshFipsEnabled": false
}
},
"links": {
```

```
"self": "admin/v2/server/security/ssh"
}
}
```

GET PowerShell Sample

```
#get Server SSH Security Settings
Write-Output "Get Server SSH Settings"
Write-Output "-----"
$serverSSH = Invoke-RestMethod -Uri "$baseURL/v2/server/security/ssh" -Method
'GET' -Headers $authHeaderWrite-Output $serverSSH | ConvertTo-Json
foreach ($server in $serverSSH.data)
{
Write-Output ("Server $($serverSSH.data)")
}
```

Method & URL

`PATCH https://[server URL]:[port]/admin/v2/server/security/ssh`

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/server/security/ssh HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "sshServerSecurity",
    "id": "1",
    "attributes": {
      "sshFipsEnabled": true
    }
  },
  "links": {
    "self": "admin/v2/server/security/ssh"
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

PATCH PowerShell Sample

```
###(PATCH) SSH Security Settings (enable FIPS)
Write-Output "Server SSH Enable FIPS Patch"
Write-Output "-----"
$update =
'{
"data": {
"type": "sshServerSecurity",
"id": "1",
"attributes": {
"sshFipsEnabled": true
}
},
"links": {
"self": "admin/v2/server/security/ssh"
}
}'$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json
-Depth 10
$patchReturn = Invoke-RestMethod
-Uri "$baseURL/v2/server/security/ssh"
-Method 'PATCH'
-Headers $authHeader
-Body $update
```

Endpoint: /server/reports

Returns the DPIA and PCI Compliance reports in JSON format.

- GET DPIA
- GET PCICompliance

Method & URL

```
GET https://[server URL]:[port]/admin/v2/server/reports/DPIA
```

GET Body Sample

```
GET https://{{host}}/admin/v2/server/reports/DPIA HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
"data": {
"attributes": {
"dpia": [{
"articles": [{
"desc": "The processing of personal data falls within Article 2's definition of material scope.
Risk is increased only if set to unknown scope.",
"name": "Material scope",
"num": 2,
"score": 1,
"value": "Unknown or undefined"},{
"desc": "Specifies the territorial scope your organization has identified in context with this application's usage.",
"name": "Territorial scope",
"num": 3,
"score": 1,
"value": "Unknown or undefined"},{
"desc": "If Not in Union was chosen for territorial scope then all users must have their data
```

```
subject status set to either Yes or No.",
…
}
}
```

GET PowerShell Sample

```
#get Server DPIA Report
Write-Output "Get Server DPIA Report"
Write-Output "-----"
$server DPIA = Invoke-RestMethod -Uri "$baseURL/v2/server/reports/DPIA"
-Method 'GET' -Headers $authHeader
Write-Output $serverDPIA | ConvertTo-Json -Depth 20
foreach ($server in $serverDPIA.data)
{
Write-Output ("Server $($serverDPIA.data)")
}
```

Method & URL

> **NOTE:** This is a REST API v1 endpoint.

```
GET https://[server URL]:
[port]/admin/v1/server/reports/PCICompliance
```

GET Body Sample

```
GET https://{{host}}/admin/v1/server/reports/PCICompliance HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
HTTP/1.1 200 OKDate: Tue, 09 Aug 2022 17:30:22 GMTContent-Type: application/vnd.api+json
Content-Length: 234 Cache-Control: no-cache, no-store, must-revalidateExpires:
-1X-Content-Type-Options: nosniffX-XSS-Protection: 1; mode=blockContent-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer{
```

```
"PCICompliance": [{"failed": 12,"passed": 12,"siteId": "e82de253-b8ec-4b70-a72d-
d017c3317f01",
"siteName": "MySite","warnings": 6},{"failed": 6,"passed": 11,"siteId": "ff493a39-1e28-
40c5-ab18-2e6a4f33f296",
"siteName": "PCI_SITE","warnings": 5}]}
```


GET PowerShell Sample

```
#get Server PCIC Report
Write-Output "Get Server PCIC Report"
Write-Output "-----"
$serverPCIC = Invoke-RestMethod -Uri "
$baseURL/v1/server/reports/PCICompliance" -Method 'GET' -Headers
$authHeaderWrite-Output $serverPCIC | ConvertTo-Json -Depth 20
foreach ($server in $serverPCIC.data)
{
Write-Output ("Server $($serverPCIC.data)")
}
```

Endpoint: /server/admin-users

Returns list of EFT admin users and creates new admin users.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/server/admin-users
```

GET Body Sample

```
GET https://{{host}}/admin/v2/admin-users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
"data": [
{
"id": "59774c12-870d-5560-a44a-c5b35cf68d4c",
"type": "adminUser",
"attributes": {
"name": "admin"
}
},
{
"id": "b76a1d7b-c3ad-5ac4-8636-06ce71ba3af3",
"type": "adminUser",
"attributes": {
"name": "Local computer\\Administrators"
}
}
],
"links": {
"self": "admin/v2/admin-users"
```

```
}
}
```

GET POWERSHELL SAMPLE

```
#get Server admin users
Write-Output "Get Server admin users"
Write-Output "-----"
$serverAdmins = Invoke-RestMethod -Uri "$baseURL/v2/admin-users" -Method 'GET' -Headers
$authHeader
Write-Output $serverAdmins | ConvertTo-Json
foreach ($server in $serverAdmins.data)
{
    Write-Output ("Server $($serverAdmins.data)")
}
```

Method & URL

`POST https://[server URL]:[port]/admin/v2/server/admin-users`

POST Body Sample

```
POST https://{{host}}/admin/v2/admin-users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
  "data": {
      "attributes": {
      "name": "Test_admin2",
      "password": "test",
      "adminConsolePermissions": {
        "accountPolicy": "server",
        "enableCom": true,
        "enableEditingAndReporting": true,
        "enablePersonalDataAccess": true
      },
      "restPermissions": {
```

```
        "enabled": true,
        "restAdminRole": true
      }
    }
  }
}
```

POST Response Body Sample

```
HTTP/1.1 201 Created Date: Tue, 09 Aug 2022 18:18:00 GMT Content-Type:
application/vnd.api+json ETag: "BF7E8C0E"

Content-Length: 394 Cache-Control: no-cache, no-store, must-revalidate Expires: -1 X-
Content-Type-Options:

nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self'
'unsafe-inline'

'unsafe-eval' data:; Referrer-Policy: no-referrer

{ "data":

{ "id": "9693cbcf-d4a9-49ac-aa1c-59efd91a692b", "type": "adminUser", "attributes": {
"adminConsolePermissions": {

"accountPolicy": "Server", "enableCom": true, "enableEditingAndReporting": true,
"enablePersonalDataAccess": true },

"name": "Test_admin2", "restPermissions": { "enabled": true, "restAdminRole": "server_
full_access" } } }, "links": {

"self": "/admin/v2/admin-users/9693cbcf-d4a9-49ac-aa1c-59efd91a692b" } }
```

POST PowerShell Sample

```
#POST Server Admin user (New User)

Write-Output "POST Server Admin (New Admin user)"

Write-Output "-----"

$update =

'{
  "data": {
    "id": "1",
    "attributes": {
      "name": "Test_admin",
      "password": "test",
      "adminConsolePermissions": {
```

```
        "accountPolicy": "server",
        "enableCom": true,
        "enableEditingAndReporting": true,
        "enablePersonalDataAccess": true
      },
      "restPermissions": {
        "enabled": true,
        "restAdminRole": true
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/admin-users" -Method 'POST' -Headers
$authHeader -Body $update
```

Endpoint: /server/admin-users/{adminId}

Returns EFT admin user (adminID required) information, which allows PATCH (update) and DELETE of admin user. To obtain the admin user ID, a GET request will need to be done against the admin-users endpoint prior to making this REST API request.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/server/admin-users/{adminID}
```

GET Body Sample

```
GET https://{{host}}/admin/v2/admin-users/59774c12-870d-5560-a44a-c5b35cf68d4c HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
"data": {
  "id": "59774c12-870d-5560-a44a-c5b35cf68d4c",
  "type": "adminUser",
  "attributes": {
    "adminConsolePermissions": {
      "accountPolicy": "Server",
      "enableCom": true,
      "enableEditingAndReporting": true,
      "enablePersonalDataAccess": true
     },
     "name": "admin",
     "restPermissions": {
       "enabled": true,
       "restAdminRole": "server_full_access"
     }
```

```
    }
  },
  "links": {
    "self": "admin/v2/admin-users/59774c12-870d-5560-a44a-c5b35cf68d4c"
  }
}
```

GET PowerShell Sample

```
#Get Server Admin Details when providing a Server Admin ID
Write-Output "Get Server Admin Details"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/admin-users/59774c12-870d-5560-a44a-c5b35cf68d4c" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($server in $serverAdminDetails.data)
{
    Write-Output ("Server $($serverAdminDetails.data)")
}
```

Method & URL

`PATCH https://[server URL]:[port]/admin/v2/server/admin-users/{adminID}.`

PATCH Body Sample

```
@adminID = 13564c1b-8e13-4e72-b8e0-9480fad06221
PATCH https://{{host}}/admin/v2/admin-users/{{adminID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "0",
    "attributes": {
        "adminConsolePermissions": {
        "enableCom": false,
```

```
        "enableEditingAndReporting": true,
        "enablePersonalDataAccess": true
      },
      "restPermissions": {
        "enabled": true,
        "restAdminRole": true
      }
    }
  }
}
```

PATCH PowerShell Sample

```
###
#PATCH Server Admin Details when providing a Server Admin ID
Write-Output "Server Admin User Patch"
$adminID = "13564c1b-8e13-4e72-b8e0-9480fad06221"
Write-Output "Admin ID: $adminID"
Write-Output "-----"
$update =
'{
  "data": {
    "id": "0",
    "attributes": {
        "adminConsolePermissions": {
        "enableCom": false,
        "enableEditingAndReporting": true,
        "enablePersonalDataAccess": true
      },
      "restPermissions": {
        "enabled": true,
        "restAdminRole": true
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
```

```
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/admin-users/$adminID" -Method 'PATCH'
-Headers $authHeader -Body $update
```

Method & URL

`DELETE https://[server URL]:[port]/admin/v2/server/admin-users/{adminID}.`

DELETE Body Sample

```
@adminID = 13564c1b-8e13-4e72-b8e0-9480fad06221
DELETE https://{{host}}/admin/v2/admin-users/{{adminID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE PowerShell Sample

```
###
#DELETE EFT admin by Admin ID
Write-Output "Server Admin DELETE"
$adminID = "f98d2a35-4d37-4891-89ed-66cb6ddf9436"
Write-Output "Admin ID: $adminID"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/admin-users/$adminID"
-Method 'DELETE' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($server in $serverAdminDetails.data)
{
    Write-Output ("Server $($serverAdminDetails.data)")
}
```

Endpoint: /server/admin-users-policy

Returns EFT admin user policies such as account and password policy. Additionally, the PATCH request allows updates to the EFT admin policies.

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/server/admin-users-policy
```

GET Body Sample

```
GET https://{{host}}/admin/v2/admin-users-policy HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": {
"id": "1",
"type": "adminUserPolicy",
"attributes": {
"accountPolicy": {
"invalidLogin": {
"account": {
               "enabled": false,
               "attemptPeriodMinutes": 5,
               "attemptRetries": 5,
               "lockoutMinutes": 30 }
               },
 "inactivity": {
 "disconnectDueToTimeout": {
 "enabled": false, "timeoutMinutes": 5},"removeInactiveAccounts": {"enabled":
false,  maxInactiveDays": 90}
 }
 },
```

```
                "passwordPolicy": {
                "complexity": {
                "enabled": false,
                "minLength": 8,
                "userNameSimilarity": {
                "enabled": true,
                "maxAllowedChars": 3 },
                "repeatingCharLimit": {
                "enabled": true,
                "maxAllowedChars": 3 },
                "characterCategories": { "enabled": true, "characterCount": 4,
"numericRequired": true,
                "upperCaseRequired": true, "lowerCaseRequired": true,
"nonAlphaNumericRequired": false,
                "non7bitAsciiRequired": false }, "forbiddenDictionary": { "enabled":
true,
                "backwardsWordsAllowed": false, "dictionaryFilePath": "" } },
                "forceResetAfterFirstLogin": false, "history": { "enabled": false,
"historyDepth": 4 },
                "reset": { "expiration": { "enabled": false, "daysToExpire": 90 } } } }
}, "links": {
                "self": "admin/v2/admin-users-policy" }
   }
```


GET PowerShell Sample

```
###
#GET Server Admin user policy
Write-Output "Get Server Admin User Policy"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/admin-users-policy" -Method
'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($server in $serverAdminDetails.data)
{
    Write-Output ("Server $($serverAdminDetails.data)")
}
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/server/admin-users-policy
```

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/admin-users-policy HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "1",
    "type": "adminUserPolicy",
    "attributes": {
      "accountPolicy": {
          "inactivity": {
          "disconnectDueToTimeout": {
            "enabled": false,
            "timeoutMinutes": 5
          }

        }
      }
    }
  }
}
```

PATCH PowerShell Sample

```
###
#PATCH Server Admin user policy (disable Admin UI disconnect)
Write-Output "Server Admin User Policy Patch"
Write-Output "-----"
$update =
'{
  "data": {
    "id": "1",
```

```
    "type": "adminUserPolicy",
    "attributes": {
      "accountPolicy": {
          "inactivity": {
          "disconnectDueToTimeout": {
            "enabled": false,
            "timeoutMinutes": 5
          }

        }
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/admin-users-policy"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /experimental/server/templates/{templateName}

> **NOTE:** Available as of EFT 8.1.0

Returns and updates the contents of the specified server template.

- GET
- PATCH

Method & URL

```
GET HTTPS://{{host}}/admin/experimental/server/templates/{templateName}
```

GET Body Sample

```
#GET Server Templates -- ##

GET https://
{{host}}/admin/experimental/server/templates/WorkspacesAdminAddedParticipantMsg.html
HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 13:17:16 GMT Content-Type:
application/vnd.api+json

Content-Length: 370 Cache-Control: no-cache, no-store, must-revalidate Expires: -1

X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:

default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer {
"data":

"<html>\r\n<body>\r\n <p>Hello %USER.LOGIN%,</p>\r\n <p>The following <b>Enhanced File
Transfer</b>

Workspace has been shared with you: %FOLDER_NAME% (owner: %WS_OWNER_NAME%).</p>\r\n

<p>Please use the following URL to access this Workspace:</p>\r\n <a
href=\"%LINK%\">%LINK%</a>

<br/><br/>\r\n \r\n %WS_MESSAGE%<br/><br/>\r\n <hr/>\r\n</body>\r\n</html>" }
```

GET PowerShell Sample

```
#####################################

#GET Server Templates -- ##

Write-Output "GET Server Templates Detail"

Write-Output "------------------------------"

#$siteID = "Enter site ID"

#$TemplateName= "WorkspacesAdminAddedParticipantMsg.html"

$TemplateDetails = Invoke-RestMethod -Uri
"$baseURL/experimental/server/templates/WorkspacesAdminAddedParticipantMsg.html" -Method
'GET' -Headers $authHeader

Write-Output $TemplateDetails | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH HTTPS://{{host}}/admin/experimental/server/templates/
{templateName}
```

PATCH Body Sample

```
###

#PATCH - Update Server template ###

PATCH https://{{host}}/admin/experimental/server/templates/PasswordResetReminderMsg.html
HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}


{

  "data": "<html>\r\n<body>\r\n HELLO USERS %USER.FULL_NAME%,<br>\r\nThe -___API TEST___
password for account:

  %USER.LOGIN% will expire in %DAYS_LEFT% days. Please change your password at your
earliest convenience.\r\n

  Instructions for changing your password via FTP, SFTP, and HTTP/S are provided below
for your convenience:<br>

  \r\n1. Please enter the following URL into your browser: %SITE.ACCOUNT_MANAGEMENT_
URL%<br>\r\n2.

  Supply your current password when prompted<br>\r\n3. Enter your new password and
confirm<br>\r\n4.

  If approved, exit the browser and login as normal<br>\r\n</body>\r\n</html>"

}
```

PATCH PowerShell Sample

```
### Update Content of Template###

### Modify Server Template - ###

Write-Output "PATCH Server Template"

Write-Output "---------------------"

$update =

'

{

  "data":  "Notice: ___PATCH TEST__The SSL certificate: %certid% is set to expire %d%
day(s) from now on

  %expirationdate%, which may impact operations or communications with the entity
associated with this certificate."

}

'



$update = $update | ConvertFrom-Json

$update = $update | ConvertTo-Json -Depth 9

$TemplateDetails = Invoke-RestMethod -Uri
"$baseURL/experimental/server/templates/SSLCertExpirationWarning.txt"

-Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /server/ha/upgrade

Note: Available as of EFT 8.1.0

The GET request returns node HA upgrade state. Additionally, the POST request changes the entire HA cluster state to the upgrade or normal state.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/server/ ha/upgrade
```

GET Body Sample

```
### GET server upgrade state ###
GET https://{{host}}/admin/v2/server/ha/upgrade HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": "notInUpgrade" }
```

GET PowerShell Sample

```
#########
#Get Server Upgrade State
Write-Output "Get Server Upgrade State: "
Write-Output "-----"
$upgradeState = Invoke-RestMethod -Uri "$baseURL/v2/server/ha/upgrade" -Method 'GET' -
Headers $authHeader
Write-Output $upgradeState | ConvertTo-Json -Depth 10
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/server/ ha/upgrade
```

POST Body Sample

```
### "Normal" state -> "Upgrade" state ###
POST https://{{host}}/admin/v2/server/ha/upgrade HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data":
    {
        "action":"begin"
    }
}
###
```

POST PowerShell Sample

```
###
#POST Server Upgrade State to “begin”
Write-Output "Server Upgrade State POST"
Write-Output "-----"
$update =
'{
    "data":
    {
        "action":"begin"
    }
}'
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/server/ha/upgrade" -Method 'POST' -
Headers
$authHeader -Body $update
```

Nodes REST API

The endpoints described in this section are related to nodes.

- Endpoint: /nodes
- Endpoint: /nodes/{nodeId}/metrics
- Endpoint: /nodes/{nodeId}/licenses
- Endpoint: /nodes/{nodeId}/licenses/{moduleName}
- Endpoint: /nodes/{nodeId}/licenses/trial-extension-challenge
- Endpoint: /nodes/{nodeId}/licenses/trial-extension-response

Endpoint: /nodes

Returns a list of EFT Nodes.

- GET

Method & URL

`GET https://[server URL]:[port]/admin/v2/nodes`

GET Body Sample

```
GET https://{{host}}/admin/v2/nodes HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": [
    {
      "type": "node",
      "id": "WIN-4NFJASSP163",
      "links": {
        "metrics": "admin/v2/nodes/WIN-4NFJASSP163/metrics"
      },
"attributes": {
  "isStarted": true,
  "isInCluster": false,
  "fullDomainName": "WIN-4NFJASSP163",
  "version": "8.0.7.4",
  "hostIps": [
    "127.0.0.1",
    "fe80::351a:6044:dfe2:f53%2"
  ] } } ], "links": { "self": "admin/v2/nodes/" } }
```

GET PowerShell Sample

```
###
#GET SERVER NODES
Write-Output "Get EFT Server Nodes"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/nodes" -Method 'GET' -Headers
$authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($server in $serverAdminDetails.data)
{
    Write-Output ("Server $($serverAdminDetails.data)")
}
```

Endpoint: /nodes/{nodeId}/metrics

Returns an EFT server's metrics, including transfers and server status. To obtain the node ID a GET request will need to be done against the /nodes endpoint prior to making this REST API request .

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/nodes/{nodeID}/metrics
```

GET Body Sample

```
GET https://{{host}}/admin/v2/nodes HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "type": "nodeMetrics",
    "id": "WIN-4NFJASSP163",
    "attributes": {
      "activity": { "activeClientDownloadBytesPerSecond": 0,
      "activeClientDownloadCount": 0,
      "activeClientUploadBytesPerSecond": 0,
      "activeClientUploadCount": 0,
      "activeServerDownloadBytesPerSecond": 0,
      "activeServerDownloadCount": 0,
      "activeServerUploadBytesPerSecond": 0,
      "activeServerUploadCount": 0,
      "connectedAdminCount": 1,
      "connectedUserCount": 0,
      "runningAwTaskCount": 0,
      "runningEventRuleCount": 0
     },
      "isInCluster": false, "isMaster": false, "isStarted": true,
```

GET PowerShell Sample

```
###
#GET SERVER NODE METRICS
Write-Output "Get EFT Server Node Metrics"
$serverNodeID = "WIN-4NFJASSP163"
Write-Output "Server Node ID: $serverNodeID"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/nodes/$serverNodeID/metrics" -
Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($server in $serverAdminDetails.data)
{
    Write-Output ("Server $($serverAdminDetails.data)")
}
```

Endpoint: /nodes/{nodeId}/licenses

Returns list of licenses on an EFT node and provides the ability to register EFT or a module.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/nodes/{nodeId}/licenses
```

GET Body Sample

```
@NodeID = WIN-4NFJASSP163
GET https://{{host}}/admin/v2/nodes/{{NodeID}}/licenses HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
"data": [
  {
    "attributes": {
      "registrationStatus": "Evaluation period"
    },
    "id": "AAMModule",
    "links": {
      "self": "admin/v2/nodes/WIN-4NFJASSP163/licenses/AAMModule"
    },
     "type": "license" }, { "attributes": { "registrationStatus": "Evaluation period" },
"id": "ARMModule",
     "links": { "self": "admin/v2/nodes/WIN-4NFJASSP163/licenses/ARMModule" }, "type":
"license" },
```

GET PowerShell Sample

```
###
```

```
#GET SERVER NODE LICENSE
Write-Output "Get EFT Server Node Licenses"
$serverNodeID = "WIN-4NFJASSP163"
Write-Output "Server Node ID: $serverNodeID"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/nodes/$serverNodeID/licenses"
-Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/nodes/
{nodeId}/licenses
```

POST Body Sample

```
@NodeID = WIN-4NFJASSP163
POST https://{{host}}/admin/v2/nodes/{{NodeID}}/licenses HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": [
    {
      "id": "ARMModule",
      "attributes": {
        "serialNumber": "MySerialNumberHere"
      }
    }
  ]
}
```

POST PowerShell Sample

```
###
#POST SERVER NODE LICENSE
Write-Output "Register EFT Server Node"
$serverNodeID = "WIN-4NFJASSP163"
```

```
Write-Output "Server Node ID: $serverNodeID"
Write-Output "-----"
$update =
'{
  "data": [
    {
      "id": "ARMModule",
      "attributes": {
        "serialNumber": "MySerialNumberHere"
      }
    }
  ]
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/nodes/$serverNodeID/licenses"
-Method 'POST' -Headers $authHeader -Body $update
```

Available options for ids:

- AAMModule (Advanced Authentication Modes)
- ARMModule (Auditing and Reporting Module)
- AS2Module (Applicability Statement 2 Module)
- AWModule (Advanced Workflow Engine Module)
- AccelerateModule (FAST Protocol – *Deprecated*)
- CloudConnectorModule (CCM – Cloud Connector Module)
- DMZGWModule (DMZ Gateway Module)
- EFTServer (EFT Server)
- EnterpriseActionsWModule (Enterprise Actions Module)
- FTPModule (FTP/S Module)
- FileTransferClientModule (File Transfer Client Module)
- FolderMonitorEventModule (Folder Monitor Event Module)
- HSModule (will be deprecated)
- HTTPModule (HTTP/s Module)
- PGPModule (OpenPGP Module)
- RAModule (Remote Agent Module)

- SSHModule (SFTP Module)
- SecureFormsModule (Secure Forms Module)
- TimerEventModule (Timer Event Module)
- WorkspacesModule (Workspaces Module)

Endpoint: /nodes/{nodeId}/licenses/{moduleName}

Returns registration status of a given module

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/nodes/{nodeId}/licenses/{moduleName}
```

GET Body Sample

```
###
#GET Module Registration Status
@moduleName = EFTServer
GET https://{{host}}/admin/v2/nodes/{{NodeId}}/licenses/{{moduleName}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "attributes": { "registrationState": "Evaluation period" }, "id":
"EFTServer", "type": "license" },
"links": { "self": "admin/v2/nodes/DTY2019WinServe/licenses/EFTServer" } }
```

GET PowerShell Sample

```
###
#GET A SERVER NODE LICENSE MODULE INFORMATION
Write-Output "Get EFT Server Node Licenses"
$serverNodeID = "DTY2019WinServe"
$licenseModule = "EFTServer"

Write-Output "License Module: $licenseModule"
Write-Output "-----"
```

```
$serverAdminDetails = Invoke-RestMethod -Uri
"$baseURL/v2/nodes/$serverNodeID/licenses/$licenseModule"

-Method 'GET' -Headers $authHeader

Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Endpoint: /nodes/{nodeId}/licenses/trial-extension-challenge

Returns trial extension challenge string

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/nodes/
{nodeId}/licenses/trial-extension-challenge
```

GET Body Sample

```
###

#GET TRIAL EXTENSION CHALLENGE

@NodeID = “DTY2019WinServe”

GET https://{{host}}/admin/v2/nodes/{{NodeId}}/licenses/trial-extension-challenge
HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "attributes": { "challengeString":
"nnPwL0AAq2304GWn0KnniO0z85owwH6xL3vw8pQm0LvdUVE10=" }, "id": "1",

"type": "trialExtension" }, "links": { "self": "admin/v2/licenses/trial-extension-
challenge" } }
```

GET PowerShell Sample

```
###

#GET TRIAL EXTENSION CHALLENGE

Write-Output "Get EFT Server Node Licenses"

$serverNodeID = "DTY2019WinServe"


Write-Output "$serverNodeID"

Write-Output "-----"
```

```
$serverAdminDetails = Invoke-RestMethod -Uri
"$baseURL/v2/nodes/$serverNodeID/licenses/trial-extension-challenge"

-Method 'GET' -Headers $authHeader

Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Endpoint: /nodes/{nodeId}/licenses/trial-extension-response

Allows the user to provide response string to extend the trial.

- POST

Method & URL

```
POST https://[server URL]:[port]/admin/v2/nodes/
{nodeId}/licenses/trial-extension-response
```

POST Body Sample

```
@NodeID = "DY-Win2019-1a"


POST https://{{host}}/admin/v2/nodes/{{NodeID}}/licenses/trial-extension-response
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "attributes": {
      "responseString":
"XN00P00PSJ00P02KE7VUE0TKW2TO6WTWTKEZTWE3W7TUF3RKFW3M3PS83PS03PS03RCPSB3RCPS83RCT"
    }
  }
}
###
```

Site Endpoints

The endpoints described in this section are related to sites.

- Endpoint: /sites
- Endpoint: /sites/status
- Endpoint: /sites/{siteId}
- Endpoint: /sites/{siteId}/metrics
- Endpoint: /sites/{siteId}/authentication
- Endpoint: /sites/{siteId}/general
- Endpoint: /sites/{siteID}/ftps
- Endpoint: /sites/{siteId}/https
- Endpoint: /sites/{siteId}/networkAndSecurity
- Endpoint: /sites/{siteId}/ipAccess
- Endpoint: /sites/{siteId}/ipAccessList/{ipAccessId}
- Endpoint: /sites/{siteId}/ipAutoBanList
- Endpoint: /sites/{siteId}/ipAutoBanList/{ipAutoBanId}
- Endpoint: /sites/{siteId}/sms
- Endpoint: /sites/{siteId}/sms/{profileName}
- Endpoint: /sites/{siteId}/accountSecurity
- Endpoint: /sites/{ siteId}/workspaces
- Endpoint: /sites/{siteId}/sendPortal
- Endpoint: /sites/{ siteId}/dropOffPortal
- Endpoint: /sites/{siteId}/privacyPolicy
- Endpoint: /sites/{siteId}/termsOfService
- Endpoint: /sites/{siteId}/gdpr
- Endpoint: /sites/{siteId}/uploadForms
- Endpoint: /sites/{siteId}/uploadForms/{uploadFormName}
- Endpoint: /sites/{siteId}/outlookDeploymentScript
- Endpoint: /sites/{siteId}/contentIntegrity
- Endpoint: /sites/{siteId}/contentIntegrity/{profileId}
- Endpoint: /sites/{siteId}/custom-commands
- Endpoint: /sites/{siteId}/custom-commands/{customCommandID}
- Endpoint: /sites/{siteId}/user-templates

- Endpoint: /sites/{siteId}/user-templates/{userTemplateid}
- Endpoint: /sites/{siteId}/user-groups
- Endpoint: /sites/{siteId}/user-groups/{groupid}
- Endpoint: /sites/{siteId}/user-groups/{groupid}/relationships/users
- Endpoint: /sites/{siteId}/ram/agents
- Endpoint: /sites/{siteId}/ram/agents/{remoteAgentID}
- Endpoint: /sites/{siteId}/ram/agents/templates
- Endpoint: /sites/{siteId}/ram/agents/templates/{remoteAgentsTemplateID}
- Endpoint:/sites/{siteId}/awe-tasks
- Endpoint:/sites/{siteId}/awe-tasks/{aweTaskID}
- Endpoint:/sites/{siteId}/awe-tasks-folders
- Endpoint:/sites/{sitetId}/awe-tasks-folders/{aweTaskFolderID}
- Endpoint: /sites/{siteId}/connection-profiles
- Endpoint: /sites/{siteId}/connection-profiles/{connectionProfileID}
- Endpoint: /experimental/site/templates/{templateName}
- Endpoint:/sites/{siteID}/dmz

Endpoint: /sites

Returns and update site(s) settings.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites
```

GET Body Sample

```
### GET SITE ###
# @name siteList

GET https://{{host}}/admin/v2/sites HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
"data": [ { "type": "site", "id": "892b16dc-24a8-473f-a74e-c597b824c879", "attributes":
{ "name":
"MySite" }, "links": { "self": "admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879",
"metrics":
"admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879/metrics" } },
{ "type": "site", "id": "5f99540a-da95-41c4-8b3c-d423848bdd46", "attributes": { "name":
"MySite2" },
"links": { "self": "admin/v2/sites/5f99540a-da95-41c4-8b3c-d423848bdd46", "metrics":
"admin/v2/sites/5f99540a-da95-41c4-8b3c-d423848bdd46/metrics" } } ], "links": { "self":
"admin/v2/sites" }
}
```

GET PowerShell Sample

```
# Get all sites
Write-Output "Site"
```

```
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites" -Method 'GET' -Headers
$authHeader
Write-Output $siteList | ConvertTo-Json
foreach ($site in $siteList.data)
{
    Write-Output ("Site  $($site.id): $($site.attributes.name)")
}

$siteID = $siteList.data[0].id
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites
```

POST Body Sample

```
#POST Create a new Site
POST https://{{host}}/admin/v2/sites HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "site",
    "attributes": {
      "pciComplianceEnabled": true,
      "siteLabel": "MySite5",
      "siteRootFolder": "C:\\InetPub\\EFTRoot\\MySite\\",
      "createUnixStyleSubFolders": true,
      "createFoldersForNewUsers": true
    }
  }
}
```

POST Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated POST request(s).

POST PowerShell Sample

```
####Added 2/01/2020
#POST Site/ (Create a new Site)
Write-Output "POST Site (Create a new Site)"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "site",
    "attributes": {
      "pciComplianceEnabled": true,
      "siteLabel": "MySite6",
      "siteRootFolder": "C:\\InetPub\\EFTRoot\\MySite\\",
      "createUnixStyleSubFolders": true,
      "createFoldersForNewUsers": true
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites" -Method 'POST' -Headers
$authHeader -Body $update
```

Endpoint:/sites/status

Returns the current status of all sites

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v1/sites/status
```

GET Body Sample

```
### GET SITE ###
# @name siteList

GET https://{{host}}/admin/v1/sites/status HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{"info":[{"nodeName":"DY-Win2019-1a","sites":[{"DMZConnected":false,"activity":
{"activeClientDownloadBytesPerSecond":0,
"activeClientDownloadCount":0,"activeClientUploadBytesPerSecond":0,"activeClientUploadCount":0,
"activeServerDownloadBytesPerSecond":0,"activeServerDownloadCount":0,"activeServerUploadBytesPerSecond":0,
"activeServerUploadCount":0,"connectedUserCount":0,"runningAWTaskCount":0,"runningEventRuleCount":0},"id":
"5ceae6e3-11b1-40c6-b4e4-3078a8e88a35","lastUserLoginTime":0,"name":"MySite","startTime":1659543775,"state":"Running"}]}]
}
```


GET PowerShell Sample

```
# Get all sites
Write-Output "Site"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v1/sites/status" -Method 'GET' -Headers $authHeader
```

```
Write-Output $siteList | ConvertTo-Json
foreach ($site in $siteList.data)
{
    Write-Output ("Site  $($site.id): $($site.attributes.name)")
}
```

Endpoint: /sites/{siteId}

Returns all site settings for the specified Site ID; To obtain the Site ID a GET request will need to be done against the /sites endpoint prior to making this request.

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteid}
```

GET Body Sample

```
### Returns all site settings for the specified Site ID ###
GET https://{{host}}/admin/v2/sites/{{Siteid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
  "data": {
"type": "site",
"id": "892b16dc-24a8-473f-a74e-c597b824c879",
"attributes": { "name": "MySite",
"general": { "authType": "EFT",
 "rootFolder": "C:\\InetPub\\EFTRoot\\MySite\\",
 "lastModifiedBy": "WIN-IKTLG8MULV9\\Administrator",
 "lastModifiedTime": 1643636803
},
"listenerSettings": {
 "accountManagementUrl": "https://172.22.150.62/manageaccount",
 "httpDomain": "172.22.150.62",
 "listenIps": [ "0.0.0.0" ],
 "ftps": { "explicitPort": 21,
 "implicitPort": 990 },
 "https": { "port": 443 },
 "sftp": { "port": 22 } },
 "workspacesSettings": { "enabled": true },
```

```
 "dmz": { "enabled": false,
 "server": [ { "nodeName": "WIN-IKTLG8MULV9",
 "ipAddresses": [ "" ],
 "port": 44500 } ] } } },
 "links": { "metrics": "admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879/metrics",
"self": "admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879" }
}
```


GET PowerShell Sample

```
####Added 2/01/2020
### Returns all site settings for the specified Site ID ###
### User must obtain the SiteID from Get Sites
Write-Output "Site"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID" -Method 'GET' -Headers
$authHeader
Write-Output $siteList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/metrics

Returns all site metrics for the specified Site ID; To obtain the Site ID a GET request will need to be done against the /sites endpoint prior to making this request.

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteid}/metrics
```

GET Body Sample

```
### GET Site Metrics ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/metrics/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "id": "4d1b02ee-5c9c-4129-bf1d-663534248b3f",
    "type": "siteMetrics",
    "attributes": {
      "name": "MySite6",
      "startTime": " 12:00:00 AM",
      "isRunning": false,
      "isDMZGatewayConnected": false,
      "definedUsers": 0,
      "disabledUserCount": 0,
      "nodes": [
        {
          "activeClientDownloadBytesPerSecond": 0,
          "activeClientDownloadCount": 0,
          "activeClientUploadBytesPerSecond": 0,
          "activeClientUploadCount": 0,
          "activeServerDownloadBytesPerSecond": 0,
          "activeServerDownloadCount": 0,
```

```
          "activeServerUploadBytesPerSecond": 0,
          "activeServerUploadCount": 0,
          "connectedUserCount": 0,
          "name": "WIN-IKTLG8MULV9",
          "runningAWTaskCount": 0,
          "runningEventRuleCount": 0
        }
      ]
    }
  },
  "links": {
    "self": "admin/v2/sites/4d1b02ee-5c9c-4129-bf1d-663534248b3f/metrics"
  }
}
```


GET PowerShell Sample

```
### Returns all site Metrics for the specified Site ID ###
### User must obtain the SiteID from Get Sites
Write-Output "Site Metrics"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/metrics" -Method 'GET' -
Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/authentication

Returns current authentication settings for the Site ID specified on the request; To obtain the Site ID a GET request will need to be done against the /sites endpoint prior to making this request.

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteid}/authentication
```

GET Body Sample

```
### GET Site Authentication Provider (EFT, AD, LDAP, ODBC) ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/authentication/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "id": "3e2cae3a-db0f-44bd-812d-4ca6b0f04c91",
    "type": "siteAuthentication",
    "attributes": {
      "advancedAuth": {},
      "userAuth": {
        "type": "LDAP",
        "ldap": {
          "advanced": {
            "ldapVersion": {
              "enabled": true,
              "version": 3
            },
            "overrideSearchPage": {
              "enabled": true,
```

```
      "size": 1000
    },
    "referralChasingEnabled": false,
    "searchScope": {
      "enabled": true,
      "level": 2
    },
    "serverSidePageControlEnabled": true,
    "timeOut": {
      "enabled": true,
      "seconds": 60
    },
    "userAttributes": {
      "enabled": true,
      "value": {
        "custom1": [],
        "custom2": [],
        "custom3": [],
        "email": [
          "mail",
          "email"
        ],
        "fullName": [
          "name",
          "cn"
        ],
        "settingTemplate": []
      }
    }
  },
  "host": {
    "attribute": "cn",
    "baseDn": "",
    "port": 389,
    "server": "",
    "userFilter": "(objectClass=person)"
  },
```

```
          "onlySyncUserOnFirstLogin": false,
          "refreshInterval": {
            "inherited": true,
            "enabled": 0,
            "minutes": 0
          },
          "useSsl": false,
          "user": {
            "name": "",
            "password": ""
          }
        }
      }
    }
  },
  "links": {
    "self": "/admin/v2/sites/3e2cae3a-db0f-44bd-812d-4ca6b0f04c91/authentication"
  }
}
```


GET PowerShell Sample

```
####Added 2/02/2022
### GET Site Authentication Provider (EFT, AD, LDAP, ODBC) ###
### User must obtain the SiteID from Get Sites
Write-Output "Site Authentication Provider "
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/authentication" -Method
'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteid}/authentication
```

PATCH Body Sample

```
###This example will Set ODBC as the Authentication type and enable radius
#PATCH Site Authentication type
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/authentication/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
  "data": {
    "id": "",
    "type": "site",
    "attributes": {
      "userAuth": {
        "type": "ODBC",
        "odbc": {
          "connectionString": "Provider=MSDASQL;SERVER=;DATABASE=ODBC;UID=sa;PWD= ",
          "encryptUserPassword": true,
          "refreshInterval": {
            "inherited": true,
            "enabled": false,
            "minutes": 0
          }
        }
      },
      "advancedAuth": {
        "type": "radius",
        "radius": {
          "server": "",
          "port": 0,
          "nasIdentifier": "",
          "sharedSecret": "",
          "connectionRetries": 0,
          "timeOutSeconds": 0
        }
      }
    }
  }
}
```

PATCH PowerShell Sample

```
###This example will Set ODBC as the Authentication type and enable radius
#PATCH Site Authentication type
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/authentication/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
  "data": {
    "id": "",
    "type": "site",
    "attributes": {
      "userAuth": {
        "type": "ODBC",
        "odbc": {
          "connectionString": "Provider=MSDASQL;SERVER=;DATABASE=ODBC;UID=sa;PWD= ",
          "encryptUserPassword": true,
          "refreshInterval": {
            "inherited": true,
            "enabled": false,
            "minutes": 0
          }
        }
      },
      "advancedAuth": {
        "type": "radius",
        "radius": {
          "server": "",
          "port": 0,
          "nasIdentifier": "",
          "sharedSecret": "",
          "connectionRetries": 0,
          "timeOutSeconds": 0
        }
      }
    }
  }
```

```
}
```

Endpoint: /sites/{siteId}/general

Returns and update the site general settings.

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/general
```

GET Body Sample

```
### GET Site General Settings ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/general/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "type": "siteGeneral",
    "attributes": {
      "overrideVfsCredentials": {
        "enabled": false,
        "value": {
          "login": "",
          "password": ""
        }
      },
      "siteRootFolder": "C:\\InetPub\\EFTRoot\\MySite\\"
    }
  },
  "links": {
    "self": "/admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879/general"
```

```
  }
}
```

GET PowerShell Sample

Note: As of EFT 8.1.0 the general REST API endpoint will also return any VFS Site Root folder configuration details when the site root has been configured in the cloud.

```
### GET Site General Settings###
### User must obtain the SiteID from Get Sites
Write-Output "Site General Settings"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/general" -Method 'GET' -
Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/general
```

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/general/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "",
    "type": "",
    "attributes": {
      "siteRootFolder": "C:\\InetPub\\EFTRoot\\MySite\\",
      "overrideVfsCredentials": {
        "enabled": true,
```

```
        "value": {
          "login": "test",
          "password": "passwordtest"
        }
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
{
  "data": {
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "type": "siteGeneral",
    "attributes": {
      "overrideVfsCredentials": {
        "enabled": true,
        "value": {
          "login": "test",
          "password": "cGFzc3dvcmR0ZXN0"
        }
      },
      "siteRootFolder": "C:\\InetPub\\EFTRoot\\MySite\\"
    }
  },
  "links": {
    "self": "/admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879/general"
  }
}
```

PATCH PowerShell Sample

```
### PATCH Site General Settings###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH Site General Settings"
Write-Output "-----"
$update =
'{
  "data": {
    "id": "",
    "type": "",
    "attributes": {
      "siteRootFolder": "C:\\InetPub\\EFTRoot\\MySite\\",
      "overrideVfsCredentials": {
        "enabled": true,
        "value": {
          "login": "test",
          "password": "passwordtest"
        }
      }
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/general" -Method
'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteID}/ftps

Returns and update the FTP(s) settings

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ftps
```

GET Body Sample

```
### GET Site FTP(s) Settings ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ftps/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
  "data": {
    "type": "site",
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "attributes": {
      "ftp": {
        "enabled": false,
        "port": 21
      },
      "explicitFtps": {
        "enabled": true,
        "port": 21
      },
      "implicitFtps": {
        "enabled": true,
        "port": 990
      },
```

```
      "ftpConfig": {
        "enableClearCommandChannel": false,
        "enableFtpClientAntiTimeout": true,
        "enableIntegrityChecking": true,
        "enableMultiPartTransfers": true,
        "enableSiteToSiteTransfer": false,
        "enableUnprotectedDataChannel": false,
        "enableUtf8Encoding": false,
        "messageOverride": {
          "connectionMsg": "EFT Login - %DATE% %TIME% - Please enter valid credentials
to continue",
          "userLimitReachedMsg": "",
          "quitSessionMsg": ""
        },
        "passiveMode": {
          "enabled": false,
          "value": {
            "ipAddress": "0.0.0.0",
            "portRangeFrom": 28000,
            "portRangeTo": 30000
          }
        }
      }
    }
  },
  "links": {
    "self": "/admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879/ftps"
  }
}
```


GET PowerShell Sample

```
### GET Site FTP(S) Settings###
### User must obtain the SiteID from Get Sites
Write-Output "Site FTP(S) Settings"
Write-Output "----"
```

```
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ftps" -Method 'GET' -
Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/general
```

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/ftps/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes":{
      "ftp": {
        "enabled": true,
        "port": 10
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
{
  "data": {
    "type": "site",
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "attributes": {
```

```
      "ftp": {
        "enabled": true,
        "port": 10
      },
      "explicitFtps": {
        "enabled": true,
        "port": 10
      },
      "implicitFtps": {
        "enabled": true,
        "port": 990
      },
      "ftpConfig": {
        "enableClearCommandChannel": false,
        "enableFtpClientAntiTimeout": true,
        "enableIntegrityChecking": true,
        "enableMultiPartTransfers": true,
        "enableSiteToSiteTransfer": false,
        "enableUnprotectedDataChannel": false,
        "enableUtf8Encoding": false,
        "messageOverride": {
          "connectionMsg": "EFT Login - %DATE% %TIME% - Please enter valid credentials
to continue",
          "userLimitReachedMsg": "",
          "quitSessionMsg": ""
        },
        "passiveMode": {
          "enabled": false,
          "value": {
            "ipAddress": "0.0.0.0",
            "portRangeFrom": 28000,
            "portRangeTo": 30000
          }
        }
      }
    }
  },
  "links": {
```

```
    "self": "/admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879/ftps"
  }
}
```

PATCH PowerShell Sample

```
### PATCH FTP(S) Settings###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH FTP(S) Settings"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes":{
      "ftp": {
        "enabled": true,
        "port": 25
      }
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ftps"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/https

Returns and update the HTTP(s) settings

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/https
```

GET Body Sample

```
### GET Site HTTP(s) Settings ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/https/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "type": "site",
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "attributes": {
      "http": {
        "enabled": false,
        "port": 80
      },
      "https": {
        "enabled": true,
        "port": 411
      },
      "domain": "172.22.150.62",
      "enableRestPage": false,
      "redirectHttpToHttps": false,
      "enableHsts": true,
```

```
      "allowWebServices": false,
      "as2": {
        "enabled": false,
        "id": "",
        "cert": {
          "passPhrase": true,
          "privateKeyPath": "",
          "publicKeyPath": ""
        }
      },
      "mfa": {
        "enabled": false,
        "type": "email"
      },
      "mtc": {
        "enabled": true,
        "value": {
          "enableFileCache": true,
          "enableFileOpenInExternalApps": true,
          "enableFileSharing": true,
          "enableFilesSavingToVault": true,
          "enableSavingProfilePassword": true
        }
      }
    }
  },
  "links": {
    "self": "/admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879/https"
  }
}
```


GET PowerShell Sample

```
### GET Site HTTP(s) Settings###
### User must obtain the SiteID from Get Sites
Write-Output "Site HTTPS(S) Settings"
```

```
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/https" -Method 'GET' -
Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/https
```

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/https/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes":{
      "https": {
        "enabled": true,
        "port": 490
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
{
  "data": {
    "type": "site",
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "attributes": {
      "http": {
```

```
        "enabled": false,
        "port": 80
      },
      "https": {
        "enabled": true,
        "port": 490
      },
      "domain": "172.22.150.62",
      "enableRestPage": false,
      "redirectHttpToHttps": false,
      "enableHsts": true,
      "allowWebServices": false,
      "as2": {
        "enabled": false,
        "id": "",
        "cert": {
          "passPhrase": true,
          "privateKeyPath": "",
          "publicKeyPath": ""
        }
      },
      "mfa": {
        "enabled": false,
        "type": "email"
      },
      "mtc": {
        "enabled": true,
        "value": {
          "enableFileCache": true,
          "enableFileOpenInExternalApps": true,
          "enableFileSharing": true,
          "enableFilesSavingToVault": true,
          "enableSavingProfilePassword": true
        }
      }
    }
  },
```

```
  "links": {
    "self": "/admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879/https"
  }
}
```

Endpoint: /sites/{siteId}/networkAndSecurity

Returns and update the network and security settings.

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/networkandsecurity/
```

GET Body Sample

```
### GET Site Network and Security Settings ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/networkandsecurity/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "type": "site",
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "attributes": {
      "connectionLimits": {
        "maxTransferSpeed": false,
        "maxConcurrentSocketConnections": false,
        "maxConcurrentLogins": false,
        "maxConnectionsPerUser": false,
        "maxConnectionFromSameIP": false
      },
      "autoBan": {
        "enabled": true,
        "value": {
          "banIfExcessiveInvalidCmdsReceived": true,
          "banIpsPermanently": false,
```

```
          "numberOfInvalidCmds": 5,
          "sensitivityLevel": "Medium"
        }
      }
    }
  },
  "links": {
    "self": "/admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879/networkAndSecurity"
  }
}
```

GET PowerShell Sample

```
####Added 2/03/2022
### GET Site Network and Security Settings###
### User must obtain the SiteID from Get Sites
Write-Output "GET Site Network and Security Settings"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/networkandsecurity" -
Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/1networkandsecurity/
```

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/networkandsecurity/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
```

```
      "connectionLimits": {
        "maxConcurrentLogins": true,
        "maxConcurrentSocketConnections": true,
        "maxConnectionFromSameIP": true,
        "maxConnectionsPerUser": true,
        "maxTransferSpeed": true
      },
      "denialOfService": {
        "autoBan": {
          "enabled": true,
          "value": {
            "banIfExcessiveInvalidCmdsReceived": true,
            "numberOfInvalidCmds": true,
            "sensitivityLevel": "Low",
            "banIpsPermenantly": true
          }
        }
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
HTTP/1.1 200 OK Date: Thu, 25 Aug 2022 18:58:06 GMT Content-Type:
application/vnd.api+json ETag: "88131696"

Content-Length: 663 Cache-Control: no-cache, no-store, must-revalidate Expires: -1

X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self'

'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer { "data": { "type":
"site", "id":

"c9551b5d-f904-4612-b690-d51bfde2eb1f", "attributes": { "connectionLimits": {
"maxTransferSpeed": true,

"maxTransferSpeedValue": 820, "maxConcurrentSocketConnections": true,
"maxConcurrentSocketConnectionsValue": 10,
```

```
"maxConcurrentLogins": true, "maxConcurrentLoginsValue": 10, "maxConnectionsPerUser":
true,
"maxConnectionsPerUserValue": 1, "maxConnectionFromSameIP": true,
"maxConnectionFromSameIPValue": 1 },
"autoBan": { "enabled": true, "value": { "banIfExcessiveInvalidCmdsReceived": true,
"banIpsPermanently": false, "numberOfInvalidCmds": 5, "sensitivityLevel": "Medium" } } }
}, "links": { "self":
"/admin/v2/sites/c9551b5d-f904-4612-b690-d51bfde2eb1f/networkAndSecurity" } }
```


PATCH PowerShell Sample

```
##Patch SITE Network Security settings
Write-Output "Site Network Security PATCH"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes": {
      "connectionLimits": {
        "maxConcurrentLogins": true,
        "maxConcurrentSocketConnections": true,
        "maxConnectionFromSameIP": true,
        "maxConnectionsPerUser": true,
        "maxTransferSpeed": true
      },
      "denialOfService": {
        "autoBan": {
          "enabled": true,
          "value": {
            "banIfExcessiveInvalidCmdsReceived": true,
            "numberOfInvalidCmds": true,
            "sensitivityLevel": "Low",
            "banIpsPermenantly": true
          }
        }
      }
```

```
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchNSReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/networkandsecurity" -
Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $patchNSReturn | ConvertTo-Json
```

Endpoint: /sites/{siteId}/ipAccess

Returns and update the network and security Site IP access/ban list Settings.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/ipAccessList
```

GET Body Sample

```
### GET Site IP access/ban list Settings ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ipAccessList HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": [
    {
      "id": "192.168.100.*",
      "type": "access",
      "attributes": {
        "accessType": "Allow",
        "date": "2022-02-04",
        "isAutoBan": false,
        "reason": "Allow for test",
        "sequenceNumber": 1
      }
    },
    {
      "id": "0.0.0.0",
      "type": "access",
      "attributes": {
        "accessType": "Deny",
```

```
        "date": "1969-12-31",
        "isAutoBan": true,
        "reason": "",
        "sequenceNumber": 2
      }
    }
  ],
  "links": {
    "self": "/admin/v2/sites/a70ccebd-1317-4992-84e7-bb4cbddc02e4/ipAccessList"
  }
}
```

GET PowerShell Sample

```
### GET Site IP access/ban list Settings###
### User must obtain the SiteID from Get Sites
Write-Output "GET Site IP access/ban list Settings"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ipAccessList" -Method
'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/
{siteId}/ipAccessList
```

POST Body Sample

```
POST https://{{host}}/admin/v2/sites/{{Siteid}}/ipAccessList HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "139:10:112:56::246",
```

```
    "type": "access",
    "attributes": {
      "accessType": "Allow",
      "reason": "API TEST",
      "sequenceNumber": 4
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
{
  "data": {
    "id": "139:10:112:56::246",
    "type": "access",
    "attributes": {
      "accessType": "Allow",
      "date": "2022-02-04",
      "isAutoBan": false,
      "reason": "API TEST",
      "sequenceNumber": 4
    }
  },
  "links": {
    "self": "/admin/v2/sites/a70ccebd-1317-4992-84e7-
bb4cbddc02e4/ipAccessList/139:10:112:56::246"
  }
}
```

PATCH PowerShell Sample

```
### POST Site IP access/ban list Settings###
### User must obtain the SiteID from Get Sites
```

```
Write-Output "POST Site IP access/ban list Settings"
Write-Output "-----"
$update =
'
{
  "data": {
    "id": "139:10:112:57::246",
    "type": "access",
    "attributes": {
      "accessType": "Allow",
      "reason": "API TEST",
      "sequenceNumber": 5
    }
  }
}
'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ipAccessList"
-Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/ipAccessList/{ipAccessId}

Returns, update and deletes network and security Site IP access/ban list Settings for the specified IP.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ipAccessList/ipAccessId
```

GET Body Sample

```
### GET Site IP access/ban Settings For specific IP###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ipAccessList/{{ipAccessId}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
  "data": {
    "id": "139:10:112:56::246",
    "type": "access",
    "attributes": {
      "accessType": "Allow",
      "date": "2022-02-04",
      "isAutoBan": false,
      "reason": "API TEST",
      "sequenceNumber": 2
    }
  },
  "links": {
```

```
    "self": "/admin/v2/sites/a70ccebd-1317-4992-84e7-
bb4cbddc02e4/ipAccessList/139:10:112:56::246"
  }
}
```

GET PowerShell Sample

```
####Added 2/07/2022
### GET Site IP access/ban Settings For specific IP ###
### User must obtain the SiteID from Get Sites
Write-Output "GET Site IP access/ban list Settings For specific IP "
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ipAccessList/$ipAccessId"
-Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/ipAccessList/ipAccessList/{ipAccessId}
```

PATCH Body Sample

```
## PATCH Site Network and Security Settings For specific IP###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/ipAccessList/{{ipAccessId}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "139:10:112:56::247",
    "attributes": {
      "accessType": "Allow",
      "reason": "This is a test for API PATCH on IP",
      "sequenceNumber": 2
    }
  }
```

```
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
{ "data": { "id": "139:10:112:56::247", "type": "access", "attributes": { "accessType":
"Allow",
"date": "2022-02-07", "isAutoBan": false, "reason": "This is a test for API PATCH on
IP",
"sequenceNumber": 2 } }, "links": { "self": "/admin/v2/sites/
a70ccebd-1317-4992-84e7-bb4cbddc02e4/ipAccessList/139:10:112:56::247" } }
```

PATCH PowerShell Sample

```
### PATCH Site Network and Security Settings For specific IP###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH Site Network and Security Settings For specific IP"
Write-Output "-----"
$update =
'{
  "data": {
    "id": "139:10:112:56::247",
    "attributes": {
      "accessType": "Allow",
      "reason": "This is a test for PS PATCH on IP",
      "sequenceNumber": 2
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ipAccessList/$ipAccessId"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/
{siteId}/ipAccessList/{ipAccessId}
```

DELETE Body Sample

```
### DELETE Site IP access/ban Settings For specific IP###

DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/ipAccessList/{{ipAccessId}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Tue, 09 Aug 2022 20:34:49 GMT Content-Length: 0 Cache-
Control: no-cache,

no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection:
1;

mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;

Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
####Added 2/07/2022

### DELETE Site IP access/ban Settings For specific IP ###

### User must obtain the SiteID from Get Sites

### User must obtain the IP id to be deleted ###

Write-Output "DELETE Site IP access/ban Settings For specific IP ###"

Write-Output "----"

#$siteID = Enter SiteID here

$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ipAccessList/$ipAccessId"

-Method 'DELETE' -Headers $authHeader

Write-Output $siteList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/ipAutoBanList

Returns information about the Auto-banned Ips list

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/ipAutoBanList
```

GET Body Sample

```
### GET Autoban List###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ipAutoBanList HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{"data":[{"id":"10.91.160.139","type":"accessBan"}],"links":{"self":"/admin/
v2/sites/5ceae6e3-11b1-40c6-b4e4-3078a8e88a35/ipAutoBanList"}}
```

GET PowerShell Sample

```
$siteID = $siteList.data[0].id


####Added 2/01/2020
### Returns all site auto ban list###
Write-Output "Site Auto Ban List"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/IpAutoBanList" -Method
'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/ipAutoBanList/{ipAutoBanId}

Remove a specific IP from the Auto-banned IP list

- DELETE

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/
{siteId}/ipAccessList{ipAutoBanId)
```

DELETE Body Sample

```
@banId = {{banList.response.body.$.data[0].id}}

### GET Autoban List###
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/ipAutoBanList/{{banId}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content
Date: Thu, 04 Aug 2022 19:43:37 GMT
Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate
Expires: -1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
$banID = $banList.data[0].id
```

```
$banList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/IpAutoBanList/$banID" -
Method 'DELETE' -Headers $authHeader

Write-Output $banList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/sms

Returns and updates the SMS configuration for the site.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/sms
```

GET Body Sample

```
### GET SMS Configuration####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/sms HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": [
    {
      "id": "Twilio Generic",
      "type": "smsSettings",
      "attributes": {
        "serviceType": "twilioGeneric",
        "services": {
          "accountSid": "xxxxxxx ...",
          "authToken": "xxxxx ....",
          "twilioNumber": "+1210...",
          "message": "Your passcode is: %Account_Session_OTP%",
          "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
        },
        "proxy": {
          "enabled": false,
          "hostName": "",
          "password": "",
```

```
          "port": 8080,
          "type": 0,
          "userName": ""
        }
      }
    }
  ],
  "links": {
    "self": "/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/sms"
```


GET PowerShell Sample

```
####Added 2/08/2022 ###
###GET SMS Settings for Site###
Write-Output "GET SMS Settings for Site"
Write-Output "----"
#$siteID = "Enter site ID"
$smsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sms" -Method 'GET' -Headers $authHeader
Write-Output $smsList | ConvertTo-Json -Depth 25
```

Method & URL

`POST https://[server URL]:[port]/admin/v2/sites/{siteId}/sms`

POST Body Sample

```
### POST add an SMS profile###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/sms HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
      "name": "Test Post SMS",
      "serviceType": "genericSmsProviderProfile",
      "services": {
```

```
        "accountSid": "AAAAAAAAAAAAAAAAAAAAAAe",
        "authToken": "0dddd0dddd0dddd0dddd",
        "twilioNumber": "+1210210210",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
      },
      "proxy": {
        "enabled": true,
        "type": "192.168.100.100",
        "hostName": "testproxy",
        "port": 1443,
        "userName": "",
        "password": ""
      }
    }
  }
}
```


POST Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated POST request(s).


```
{
  "data": {
    "id": "Test Post SMS",
    "type": "smsSettings",
    "attributes": {
      "name": "Test Post SMS",
      "serviceType": "twilioGeneric",
      "services": {
        "accountSid": "AAAAAAAAAAAAAAAAAAAAAAe",
        "authToken": "0dddd0dddd0dddd0dddd",
        "twilioNumber": "+1210210210",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
```

```
      },
      "proxy": {
        "enabled": true,
        "hostName": "testproxy",
        "password": "",
        "port": 1443,
        "type": 0,
        "userName": ""
      }
    }
  },
  "links": {
    "self": "/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/smsTest Post SMS"
  }
}
  }
}
```

POST PowerShell Sample

```
### POST add a new SMS profile ###
### User must obtain the SiteID from Get Sites
Write-Output "add a new SMS profile "
Write-Output "----------------------"
$update =
'{
  "data": {
    "attributes": {
      "name": "PowerShell Example",
      "serviceType": "genericSmsProviderProfile",
      "services": {
        "accountSid": "AAAAAAAAAAAAAAAAAAAAAAe",
        "authToken": "0dddd0dddd0dddd0dddd",
        "twilioNumber": "+1210210210",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
      },
```

```
      "proxy": {
        "enabled": true,
        "type": "192.168.100.100",
        "hostName": "testproxy",
        "port": 1443,
        "userName": "TestUser",
        "password": "example"
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 25
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sms"
-Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/sms/{profileName}

Returns, updates and deletes the SMS configuration for specific profile.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/sms/
{profileName}
```

GET Body Sample

```
### GET SMS Configuration####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/sms/{profileName} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "id": "Test Post SMS",
    "type": "smsSettings",
    "attributes": {
      "name": "Test Post SMS",
      "serviceType": "twilioGeneric",
      "services": {
        "accountSid": "AAAAAAAAAAAAAAAAAAAAAAe",
        "authToken": "0dddd0dddd0dddd0dddd",
        "twilioNumber": "+1210210210",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
      },
      "proxy": {
```

```
        "enabled": true,
        "hostName": "testproxy",
        "password": "",
        "port": 1443,
        "type": 0,
        "userName": ""
      }
    }
  },
  "links": {
    "self": "/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/sms/Test Post SMS"
  }
}
```


GET PowerShell Sample

```
####Added 2/08/2022 ###
###GET specific profile SMS Configuration Details###
Write-Output "GET specific profile SMS Configuration Details"
Write-Output "----"
$profileName = "PowerShell Example"
$smsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sms/$profileName" -Method
'GET' -Headers $authHeader
Write-Output $smsList | ConvertTo-Json -Depth 25
```

Method & URL

`PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/sms/{profileName}`

PATCH Body Sample

```
### PATCH SMS specific profile ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/sms/{{profileName}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
```

```
  "data": {
    "attributes": {
      "name": "",
      "serviceType": "genericSmsProviderProfile",
      "services": {
        "accountSid": "432432432143242343 21FDGFDSG",
        "authToken": "1234567899",
        "twilioNumber": "210101010101",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
      }
    }
  }
}
```


PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).


```
{
  "data": {
    "id": "Test Post SMS",
    "type": "smsSettings",
    "attributes": {
      "name": "Test Post SMS",
      "serviceType": "twilioGeneric",
      "services": {
        "accountSid": "432432432143242343 21FDGFDSG",
        "authToken": "1234567899",
        "twilioNumber": "210101010101",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
      },
      "proxy": {
        "enabled": true,
```

```
        "hostName": "testproxy",
        "password": "",
        "port": 1443,
        "type": 0,
        "userName": ""
      }
    }
  },
  "links": {
    "self": "/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/smsTest Post SMS"
  }
}
  "data": {
    "id": "Test Post SMS",
    "type": "smsSettings",
    "attributes": {
      "name": "Test Post SMS",
      "serviceType": "twilioGeneric",
      "services": {
        "accountSid": "432432432143242343 21FDGFDSG",
        "authToken": "1234567899",
        "twilioNumber": "210101010101",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
      },
      "proxy": {
        "enabled": true,
        "hostName": "testproxy",
        "password": "",
        "port": 1443,
        "type": 0,
        "userName": ""
      }
    }
  },
  "links": {
    "self": "/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/smsTest Post SMS"
```

```
  }
}
```

PATCH PowerShell Sample

```
####Added 2/08/2022
### PATCH - Updates existing SMS profile ###
### User must obtain the SiteID from Get Sites
Write-Output "add a new SMS profile "
Write-Output "----------------------"
$profileName = "PowerShell Example"
$update =
'{
  "data": {
    "attributes": {
      "name": "",
      "serviceType": "genericSmsProviderProfile",
      "services": {
        "accountSid": "432432432143242343 21FDGFDSG",
        "authToken": "1234567899",
        "twilioNumber": "210101010101",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 25
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sms/$profileName" -
Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/sms/
{profileName}
```

DELETE Body Sample

```
### DELETE SMS specific profile###

DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/sms/{{profileName}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample


```
{ "data": [ { "id": "Twilio Generic", "type": "smsSettings", "attributes": {
"serviceType": "twilioGeneric",

"services": { "accountSid": "Aabdd54dgsb2e9357b03a", "authToken":
"0dddd2e4357fac35f10132a8ff7949ec",

"twilioNumber": "+12109414973", "message": "Your passcode is: %Account_Session_OTP%",
"postUrl":

"https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages" }, "proxy": { "enabled":
true, "hostName": "",

"password": "", "port": 8080, "type": 2, "userName": "" } } }, { "id": "Andres TEST",
"type": "smsSettings",

"attributes": { "serviceType": "twilioGeneric", "services": { "accountSid": "324423",
"authToken": "54325432542352345",

"twilioNumber": "213213132123", "message": "Your passcode is: %Account_Session_OTP%",
"postUrl":

"https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages" }, "proxy": { "enabled":
false, "hostName": "",

"password": "", "port": 8080, "type": 0, "userName": "" } } }, { "id": "PowerShell
Example", "type":

"smsSettings", "attributes": { "serviceType": "twilioGeneric", "services": {
"accountSid": "43243243214324234321FDGFDSG",

"authToken": "ABCDEFT1234567899", "twilioNumber": "210101010101", "message": "Your
passcode is: %Account_Session_OTP%",

"postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages" }, "proxy": {
"enabled": true, "hostName":

"testproxy", "password": "ZXhhbXBsZQ==", "port": 1443, "type": 0, "userName": "TestUser"
} } } ], "links": {

"self": "/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/sms" } }
```


DELETE PowerShell Sample

```
###### DELETE SMS specific profile######

Write-Output "### DELETE SMS specific profile###"

Write-Output "----"

$profileName = "PowerShell Example"
```

```
$smsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sms/$profileName" -Method
'DELETE' -Headers $authHeader

Write-Output $smsList | ConvertTo-Json -Depth 25
```

Endpoint: /sites/{siteId}/accountSecurity

Returns and updates account security configuration for specific profile

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/accountSecurity
```

GET Body Sample

```
### GET Account Security Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/accountSecurity/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "type": "siteSecurity",
    "id": "0de7387f-1506-427d-b997-e18bcdb8cbae",
    "attributes": {
      "accountPolicy": {
        "invalidLogin": {
          "ip": {
            "enabled": true,
            "attemptPeriodMinutes": 1,
            "attemptRetries": 5,
            "inCorrectLoginType": "NameOnly"
          },
          "account": {
          }
        },
        "inactivity": {
        },
```

```
        "personalDetailsConfiguration": [
        ]
      },
      "passwordPolicy": {
        "complexity": {
        },
        "PersistCredentialsForEventRuleContextVariable": true,
        "suppressForgotPwd": {
        },
        "emailLoginCredentials": {
        },
        "history": {
        },
        "reset": {
        }
      }
    }
  },
  "links": {
  }
}
```


GET PowerShell Sample

```
####Added 2/09/2022 ###
### GET Account Security Configuration Details ###
Write-Output "GET Account Security Configuration Details"
Write-Output "----"
$profileName = "PowerShell Example"
$smsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/accountSecurity" -Method
'GET' -Headers $authHeader
Write-Output $smsList | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/accountSecurity
```

PATCH Body Sample

```
### PATCH Account Security Settings ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/accountSecurity/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
  "data": {
    "attributes": {
      "accountPolicy": {
        "invalidLogin": {
          "account": {
            "enabled": true,
            "action": "Lockout",
            "attemptPeriodMinutes": 10,
            "attemptRetries": 10,
            "lockoutMinutes": 10
          },
          "ip": {
            "enabled": true,
            "attemptPeriodMinutes": 10,
            "attemptRetries": 10,
            "inCorrectLoginType": "NameOrPassword"
          }
        },
        "inactivity": {
          "removeInactiveAccounts": {
            "enabled": true,
            "action": "Delete",
            "maxInactiveDays": 10
          }
        },
        "reset": {
          "enabled": true,
          "forceResetAfterFirstLogin": true,
          "expiration": {
            "enabled": true,
            "emailUpon": true,
```

```
            "daysToExpire": 10,
            "reminderPrior": {
              "enabled": true,
              "daysBefore": 10,
              "emailUser": true
            }
          }
        }
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).


```
{ "data": { "type": "site", "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "attributes":
{ "accountPolicy": {
"invalidLogin": { "ip": { "enabled": true, "attemptPeriodMinutes": 5, "attemptRetries":
5,
"inCorrectLoginType": "NameOrPassword" }, "account": { "enabled": true, "action":
"Disable",
"attemptPeriodMinutes": 11, "attemptRetries": 5, "lockoutMinutes": 5 } }, "inactivity":
{
"removeInactiveAccounts": { "enabled": true, "action": "Delete", "maxInactiveDays": 10 }
},
"personalDetailsConfiguration": [ { "id": "Email", "displayName": "Email",
"defaultValue": "",
"isEnabled": true, "isPersonalData": true, "isModifiable": true, "isVisibleToUser": true
}, {
"id": "FullName", "displayName": "Full Name", "defaultValue": "", "isEnabled": true,
"isPersonalData": true, "isModifiable": true, "isVisibleToUser": true }, { "id":
"CompanyName",
"displayName": "Company Name", "defaultValue": "", "isEnabled": true, "isPersonalData":
false,
"isModifiable": true, "isVisibleToUser": false }, { "id": "Mobile", "displayName":
"Mobile",
```

```
"defaultValue": "", "isEnabled": true, "isPersonalData": true, "isModifiable": true,

"isVisibleToUser": true }, { "id": "Description", "displayName": "Description",
"defaultValue": "",

"isEnabled": true, "isPersonalData": false, "isModifiable": true, "isVisibleToUser":
false }, {

"id": "Phone", "displayName": "Phone", "defaultValue": "", "isEnabled": true,
"isPersonalData": true,

"isModifiable": true, "isVisibleToUser": true }, { "id": "Fax", "displayName": "Fax",
"defaultValue": "",

"isEnabled": true, "isPersonalData": true, "isModifiable": true, "isVisibleToUser": true
}, { "id": "Pager",

"displayName": "Pager", "defaultValue": "", "isEnabled": true, "isPersonalData": true,
"isModifiable": true,

"isVisibleToUser": true }, { "id": "Duns", "displayName": "DUNS", "defaultValue": "",
"isEnabled": true,

"isPersonalData": false, "isModifiable": true, "isVisibleToUser": false }, { "id":
"PartnerId",

"displayName": "Partner ID", "defaultValue": "", "isEnabled": true, "isPersonalData":
false, "isModifiable": true,

"isVisibleToUser": false }, { "id": "Custom1", "displayName": "Custom 1",
"defaultValue": "",

"isEnabled": true, "isPersonalData": false, "isModifiable": true, "isVisibleToUser":
false }, { "id": "Custom2",

"displayName": "Custom 2", "defaultValue": "", "isEnabled": true, "isPersonalData":
false, "isModifiable": true,

"isVisibleToUser": false }, { "id": "Custom3", "displayName": "Custom 3",
"defaultValue": "", "isEnabled": true,

"isPersonalData": false, "isModifiable": true, "isVisibleToUser": false }, { "id":
"Comments",

"displayName": "Comments", "defaultValue": "", "isEnabled": true, "isPersonalData":
false, "isModifiable": true,

"isVisibleToUser": false } ] }, "passwordPolicy": { "complexity": { "enabled": false,
"minLength": 8,

"userNameSimilarity": { "enabled": true, "maxAllowedChars": 3 }, "repeatingCharLimit": {
"enabled": true,

"maxAllowedChars": 3 }, "characterCategories": { "enabled": true, "characterCount": 4,
"numericRequired": true,

"upperCaseRequired": true, "lowerCaseRequired": true, "nonAlphaNumericRequired": false,
"non7bitAsciiRequired": false },

"forbiddenDictionary": { "enabled": true, "backwardsWordsAllowed": false,
"dictionaryFilePath": "" } },

"PersistCredentialsForEventRuleContextVariable": true, "suppressForgotPwd": { "enabled":
false, "domainType": "All Domains" },

"emailLoginCredentials": { "enabled": true, "emailOptions": "Both" }, "history": {
"enabled": false,

"historyDepth": 4 }, "reset": { "enabled": false, "forceResetAfterFirstLogin": true,
"expiration": {
```

```
"enabled": true, "emailUpon": true, "daysToExpire": 90, "remindPrior": { "enabled":
false, "daysBefore": 5,
"emailUser": true } } } } } }, "links": { "self":
"/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/passwordSecurity" } }
```


PATCH PowerShell Sample

```
### PATCH Account Security Configuration Details ###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH Account Security Configuration Details"
Write-Output "----------------------"
$update =
'{
  "data": {
    "attributes": {
      "accountPolicy": {
        "invalidLogin": {
          "account": {
            "enabled": true,
            "action": "Disable",
            "attemptPeriodMinutes": 3,
            "attemptRetries": 3,
            "lockoutMinutes": 3
          },
          "ip": {
            "enabled": true,
            "attemptPeriodMinutes": 3,
            "attemptRetries": 3,
            "inCorrectLoginType": "NameOrPassword"
          }
        }
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 25
```

```
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/accountSecurity"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{ siteId}/workspaces

Returns and updates workspaces settings.

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/workspaces/
```

GET Body Sample

```
### GET Workspaces - Folder Sharing Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/workspaces/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
"data": { "type": "workspaces", "id": "0de7387f-1506-427d-b997-e18bcdb8cbae",
"attributes": { "enabled": true,
"newUser": { "enabled": true, "allowedDomains": { "enabled": false, "list": [ "*.*" ] },
"deniedDomains": { "enabled": false, "list": [ "*.*" ] } }, "maxExpiration": { "value":
1, "units": "Year" },
"secondVerification": "email", "guestAccounts": { "expiration": { "enabled": true,
"action": "DeleteAccountOnly",
"daysAfterLinksExpiration": 7 }, "grantHomeFolder": true } } }, "links": { "self":
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/workspaces" } }
```

GET PowerShell Sample

```
###GET workspaces Configuration Details###
Write-Output "GET workspaces Configuration Details"
Write-Output "----"
#$siteID = "Enter site ID"
$wksList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/workspaces"
-Method 'GET' -Headers $authHeader
Write-Output $wksList | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/workspaces
```

PATCH Body Sample

```
### PATCH Workspaces - Folder Sharing Setting ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/workspaces/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "attributes": {
      "enabled": true,
      "newUsers": {
        "enabled": true,
        "allowedDomains": {
          "enabled": false
        }
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).

```
HTTP/1.1 200 OK Date: Thu, 25 Aug 2022 19:20:16 GMT Content-Type:
application/vnd.api+json ETag: "FC63C399"
Content-Length: 507 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer { "data": { "type": "workspaces", "id": "c9551b5d-f904-
4612-b690-d51bfde2eb1f",
"attributes": { "enabled": true, "newUsers": { "enabled": true, "allowedDomains": {
"enabled": false,
```

```
"list": [ "*.*" ] }, "deniedDomains": { "enabled": false, "list": [ "*.*" ] } },
"maxExpiration": {
"value": 1, "units": "Year" }, "secondVerification": "email", "guestAccounts": {
"expiration": {
"enabled": false, "action": "Disable", "daysAfterLinksExpiration": 7 },
"grantHomeFolder": false } } },
"links": { "self": "/admin/v2/sites/c9551b5d-f904-4612-b690-d51bfde2eb1f/workspaces" } }
```


PATCH PowerShell Sample

```
##Patch SITE Workspaces settings
Write-Output "Site Workspaces PATCH"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes": {
      "enabled": true,
      "newUsers": {
        "enabled": true,
        "allowedDomains": {
          "enabled": false
        }
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchWSReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/workspaces" -Method 'PATCH'
-Headers $authHeader -Body $update
Write-Output $patchWSReturn | ConvertTo-Json
```

Endpoint: /sites/{siteId}/sendPortal

Returns and updates send portal configuration for specific site

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/sendPortal
```

GET Body Sample

```
### GET Send Portal Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/sendPortal/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "sendPortal",
"attributes":
{ "enabled": true, "recipients": "UsersGuestsAnonymous", "allowedDomains": { "enabled":
false,
"list": [ "*.*" ] }, "deniedDomains": { "enabled": false, "list": [ "*.*" ] },
"reservedPath": "/send", "protocol": "https", "hostName": "172.31.223.227", "port":
"443",
"autoAttachInOutlook": { "enabled": false, "whenExceedMbytes": 10 }, "linkExpiration": {
"value": 1,
"units": "Month" }, "retainFilesAfterLinkExpiration": { "value": 0, "unit": "Day" },
"allowRepliesWithFiles": true, "sendEntireMessageSecurely": "LetUserChoose",
"outOfBandPasscode": "Sender chooses", "secondVerification": "email",
"fileRequestPortal": { "enabled": false, "reservedPath": "/request" } } },
"links": { "self": "admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/sendPortal" } }
```

GET PowerShell Sample

```
###GET Send Portal Configuration Details###
Write-Output "GET Send Portal Configuration Details"
```

```
Write-Output "-------------------------------------"

#$siteID = "Enter site ID"

$SendList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sendPortal" -Method 'GET'
-Headers $authHeader

Write-Output $Sendlist | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/sendPortal
```

PATCH Body Sample

```
### PATCH Send Portal Settings ###

PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/sendPortal/ HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "type": "sendPortal",
    "attributes": {
      "enabled": true,
      "recipients": "UsersGuestsAnonymous",
      "allowedDomains": {
        "enabled": true,
        "list": [
          "hotmail.*", "gmail.*"
        ]
      },
      "deniedDomains": {
        "enabled": true,
        "list": [
          "GSB.*"
        ]
      },
      "reservedPath": "/send",
      "protocol": "https",
      "hostName": "172.31.223.227",
```

```
      "port": "443",
      "autoAttachInOutlook": {
        "enabled": false,
        "whenExceedMbytes": 10
      },
      "linkExpiration": {
        "value": 1,
        "units": "Month"
      },
      "retainFilesAfterLinkExpiration": {
        "value": 0,
        "unit": "Day"
      },
      "allowRepliesWithFiles": true,
      "sendEntireMessageSecurely": "LetUserChoose",
      "outOfBandPasscode": "Sender chooses",
      "secondVerification": "email",
      "fileRequestPortal": {
        "enabled": false,
        "reservedPath": "/request"
      }
    }
  }
}
```


PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).


```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "sendPortal",
"attributes": { "enabled": true, "recipients": "UsersGuestsAnonymous",
"allowedDomains": { "enabled": false, "list": [ "hotmail.*", "gmail.*" ] },
"deniedDomains": { "enabled": false, "list": [ "GSB.*" ] }, "reservedPath": "/send",
"protocol": "http", "hostName": "", "port": "113", "autoAttachInOutlook": { "enabled":
false,
"whenExceedMbytes": 10 }, "linkExpiration": { "value": 1, "units": "Month" },
```

```
"retainFilesAfterLinkExpiration": { "value": 0, "unit": "Day" },
"allowRepliesWithFiles": true,
"sendEntireMessageSecurely": "LetUserChoose", "outOfBandPasscode": "Sender chooses",
"secondVerification": "email", "fileRequestPortal": { "enabled": false, "reservedPath":
"/request" } } },
"links": { "self": "/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/sendPortal" } }
```


PATCH PowerShell Sample

```
Write-Output "PATCH Send Portal Configuration Details"
Write-Output "----------------------------------------"
$update =
'{
  "data": {
    "type": "sendPortal",
    "attributes": {
      "enabled": true,
      "recipients": "UsersGuestsAnonymous",
      "allowedDomains": {
        "enabled": true,
        "list": [
          "outlook.*", "yahoo.*"
        ]
      },
      "deniedDomains": {
        "enabled": true,
        "list": [
          "GSB.*"
        ]
      },
      "reservedPath": "/send",
      "protocol": "http",
      "hostName": "12.12.12.12",
      "port": "333",
      "autoAttachInOutlook": {
        "enabled": false,
        "whenExceedMbytes": 10
      },
```

```
      "linkExpiration": {
        "value": 1,
        "units": "Month"
      },
      "retainFilesAfterLinkExpiration": {
        "value": 1,
        "unit": "Day"
      },
      "allowRepliesWithFiles": true,
      "sendEntireMessageSecurely": "LetUserChoose",
      "outOfBandPasscode": "Sender chooses",
      "secondVerification": "email",
      "fileRequestPortal": {
        "enabled": false,
        "reservedPath": "/request"
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 25
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sendPortal"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{ siteId}/dropOffPortal

Returns and updates drop off portal configuration for specific site.

- PATCH
- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/dropOffPortal
```

GET Body Sample

```
## GET Drop Off Portal Settings####

GET https://{{host}}/admin/v2/sites/{{Siteid}}/dropOffPortal/ HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "id": "df3be28b-f499-4b0a-9c53-7cee33a58161", "type": "dropOffPortal",

"attributes": { "enabled": true, "reservedPath": "/dropoff", "captcha": { "type":
"reCAPTCHA",

"value": { "siteKey": "6LeXY8ofdsfdsfdsfasq8RdygpeBeclHqrVBUd-afar",

"secretKey": "6LeXY8oUAAAAABIVq8RdygpeBeclHqrVBUd-afar" } }, "linkExpiration": {
"value": 1,

"units": "Week" }, "maxMessageSize": { "enabled": true, "mBytes": 2048 },

"sendEntireMessageSecurely": "LetUserChoose", "userEmailOption": {
"allowToEnterToEmailAddress": true,

"allowedDomains": { "enabled": true, "list": [ "*.*" ] } }, "addressBookList": [
"user2<ivan@mail.com>",

"User1<elver@mail.com>" ] } }, "links": { "self":

"admin/v2/sites/df3be28b-f499-4b0a-9c53-7cee33a58161/dropOffPortal" } }
```

GET PowerShell Sample

```
####Added 2/10/2022 ###

###GET Drop Off Portal Settings###

Write-Output "GET Drop Off Portal Settings"
```

```
Write-Output "----------------------------"
#$siteID = "Enter site ID"
$DropOfflist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/dropOffPortal"
-Method 'GET' -Headers $authHeader
Write-Output $DropOfflist | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/dropOffPortal
```

PATCH Body Sample

```
### PATCH Drop Off Portal Settings###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/dropOffPortal/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "dropOffPortal",
    "attributes": {
      "enabled": true,
      "reservedPath": "/dropoff",
      "captcha": {
        "type": "reCAPTCHA",
        "value": {
          "siteKey": "6LeXY8odfasdfdsafdsafdsfsdfdsfdsfsdfdsfds-afar",
          "secretKey": "6Ldfasdfdsafdsafsdafdsafsdasfdsafdsfsd-afar"
        }
      },
      "linkExpiration": {
        "value": 1,
        "units": "Week"
      },
      "maxMessageSize": {
        "enabled": true,
        "mBytes": 2048
      },
```

```
      "sendEntireMessageSecurely": "LetUserChoose",
      "userEmailOption": {
        "allowToEnterToEmailAddress": true,
        "allowedDomains": {
          "enabled": true,
          "list": [
            "*.*"
          ]
        }
      },
      "addressBookList": ["user2<user2@mail.com>", "User1<user2r@mail.com>"]
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "dropOffPortal",
"attributes": { "enabled": true,
"reservedPath": "/dropoff", "captcha": { "type": "reCAPTCHA", "value": { "siteKey":
"6LeXY8oUAAAAABIVq8RdygpeBeclHqrVBUd-afar", "secretKey":
"6LeXY8oUAAAAABIVq8RdygpeBeclHqrVBUd-afar" } },
"linkExpiration": { "value": 1, "units": "Week" }, "maxMessageSize": { "enabled": true,
"mBytes": 2048 },
"sendEntireMessageSecurely": "LetUserChoose", "userEmailOption": {
"allowToEnterToEmailAddress": true,
"allowedDomains": { "enabled": true, "list": [ "*.*" ] } }, "addressBookList": [] } },
"links": { "self":
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/dropOffPortal" } }
```

PATCH PowerShell Sample

```
Write-Output "PATCH Drop Off Portal Settings"
Write-Output "------------------------------"
$update =
```

```
'{
  "data": {
    "type": "dropOffPortal",
    "attributes": {
      "enabled": true,
      "reservedPath": "/dropoff",
      "captcha": {
        "type": "reCAPTCHA",
        "value": {
          "siteKey": "6LeXY8odfasdfdsafdsafdsfsdfdsfdsfsdfdsfds-afar",
          "secretKey": "6Ldfasdfdsafdsafsdafdsafsdasfdsafdsfsd-afar"
        }
      },
      "linkExpiration": {
        "value": 1,
        "units": "Week"
      },
      "maxMessageSize": {
        "enabled": true,
        "mBytes": 2048
      },
      "sendEntireMessageSecurely": "LetUserChoose",
      "userEmailOption": {
        "allowToEnterToEmailAddress": true,
        "allowedDomains": {
          "enabled": true,
          "list": [
            "*.*"
          ]
        }
      },
      "addressBookList": []
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
```

```
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/dropOffPortal"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/privacyPolicy

Returns and updates the privacy policy configuration for specific site.

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/privacyPolicy
```

GET Body Sample

```
### GET Privacy Policy  Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/privacyPolicy/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "privacyPolicy",
"attributes": { "type": "Mandatory", "values": { "preventSftpsUntilAgreed": true,
"impliedForNonSubjects": true }, "agreementPath": "", "agreementLabel": "",
"effectiveDate": "Feb 11, 2022. 01:01:39 PM" } }, "links": { "self":
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/privacyPolicy" } }
```

GET PowerShell Sample

```
####Added 2/11/2022 ###
###GET Privacy Policy  Settings###
Write-Output "GET Privacy Policy  Settings"
Write-Output "----------------------------"
#$siteID = "Enter site ID"
$PPlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/privacyPolicy"
-Method 'GET' -Headers $authHeader
Write-Output $PPlist | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/privacyPolicy
```

PATCH Body Sample

```
### PATCH Privacy Policy  Settings###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/privacyPolicy/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "privacyPolicy",
    "attributes": {
      "type": "Mandatory",
      "values": {
        "preventSftpsUntilAgreed": false,
        "impliedForNonSubjects": false
      },
      "agreementPath": "",
      "agreementLabel": "",
      "effectiveDate": "Feb 11, 2020. 01:01:39 PM"
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "privacyPolicy",
"attributes": { "type": "Mandatory", "values": { "preventSftpsUntilAgreed": false,
"impliedForNonSubjects": false }, "agreementPath": "", "agreementLabel": "",
"effectiveDate": "Feb 11, 2022. 01:01:39 PM" } }, "links": { "self":
"/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/privacyPolicy" } }
```

PATCH PowerShell Sample

```
### PATCH Privacy Policy  Settings###
### User must obtain the SiteID from Get Sites
Write-Output "Privacy Policy  Settings"
Write-Output "------------------------------"
$update =
'{
  "data": {
    "type": "privacyPolicy",
    "attributes": {
      "type": "Mandatory",
      "values": {
        "preventSftpsUntilAgreed": true,
        "impliedForNonSubjects": true
      },
      "agreementPath": "",
      "agreementLabel": "",
      "effectiveDate": "Feb 11, 2020. 01:01:39 PM"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/privacyPolicy"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/termsOfService

Returns and updates the terms of service configuration for specific site

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/termsOfService
```

GET Body Sample

```
### GET Terms of Services Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/termsOfService/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "termsOfService",
"attributes": { "type": "Disabled", "agreementPath": "", "agreementLabel": "",
"effectiveDate": "Dec 16, 1950. 10:05:17 AM" } }, "links": { "self":
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/termsOfService" } }
```

GET PowerShell Sample

```
###GET terms Of Service Settings###
Write-Output "GET GET terms Of Service Settings"
Write-Output "----------------------------"
#$siteID = "Enter site ID"
$TOSlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/termsOfService"
-Method 'GET' -Headers $authHeader
Write-Output $TOSlist | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/termsOfService
```

PATCH Body Sample

```
### PATCH Terms of Services Settings###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/termsOfService/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "type": "termsOfService",
    "attributes": {
      "type": "Mandatory",
      "values": {
        "preventSftpsUntilAgreed": true
      },
      "agreementPath": "",
      "agreementLabel": "",
      "effectiveDate": "Dec 16, 2000. 10:05:17 AM"
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "termsOfService",
"attributes": { "type": "Mandatory", "values": { "preventSftpsUntilAgreed": true },
"agreementPath": "", "agreementLabel": "", "effectiveDate": "Feb 11, 2022. 01:01:53 PM"
} },
"links": { "self": "admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/termsOfService"
} }
```

PATCH PowerShell Sample

```
####Added 2/11/2022
### PATCH terms Of Service Settings###
### User must obtain the SiteID from Get Sites
Write-Output "terms Of Service Settings"
Write-Output "-------------------------"
$update =
'{
  "data": {
    "type": "termsOfService",
    "attributes": {
      "type": "Mandatory",
      "values": {
        "preventSftpsUntilAgreed": true
      },
      "agreementPath": "",
      "agreementLabel": "",
      "effectiveDate": "Dec 16, 2000. 10:05:17 AM"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/termsOfService"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/gdpr

Returns and updates the GDPR configuration for specific profile

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/gdpr
```

GET Body Sample

```
### GET the GDRP Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/gdpr/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "gdpr",
"attributes": { "materialScope": "Unknown or undefined", "territorialScope": {
"type": "Unknown or undefined", "value": { "showEUStatus": false,
"allUsersToChangeEUSubject": false } }, "processingPrinciples": "Unknown or undefined",
"lawfulnessOfProcessing": "Unknown or undefined", "conditionsForConsent":
"Unknown or undefined", "ageRestrictions": "Unknown or undefined",
"transparentInformation":
"Unknown or undefined", "directCollection": "Unknown or undefined",
"indirectCollection":
"Unknown or undefined", "rightOfAccess": "Unknown or undefined", "rightToRectify":
"Unknown or undefined", "rightToBeForgotten": "Unknown or undefined", "rightToRestrict":
"Unknown or undefined", "rightToBeNotified": "Unknown or undefined", "rightToExport":
"Unknown or undefined", "rightToObject": "Unknown or undefined", "encryption":
"Personal data is encrypted by EFT", "limitedAccess": "Configured By EFT", "purpose": {
"type": "Configured By EFT", "reason": "" }, "necessity":
{ "type": "Configured By EFT", "reason": "" }, "riskAssessment": "EFT generated DPIA
report",
"riskMitigation": { "type": "Configured By EFT", "reason": "" },
"dpoAssigned": { "type": "Configured By EFT", "email": "" },
"transferSafeguard": "Configured By EFT" } }, "links": { "self":
```

```
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/termsOfService" } }
```

GET PowerShell Sample

```
###GET GDRP Settings###
Write-Output "GET GDRP Settings"
Write-Output "-----------------"
#$siteID = "Enter site ID"
$GDPRlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/gdpr"
-Method 'GET' -Headers $authHeader
Write-Output $GDPRlist | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/gdpr
```

PATCH Body Sample

```
###PATCH the GDRP Settings###
PATCH  https://{{host}}/admin/v2/sites/{{Siteid}}/gdpr/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "gdpr",
    "attributes": {
      "materialScope": "In scope",
      "territorialScope": {
        "type": "In Union, all subjects in scope (3.1)",
        "value": {
          "showEUStatus": true,
          "allUsersToChangeEUSubject": true
        }
      },
      "processingPrinciples": "General guidance not yet met",
      "lawfulnessOfProcessing": "Data subject consent (6.1.a)",
      "conditionsForConsent": "Set via EFT's ToS or Privacy Policy",
```

```
      "ageRestrictions": "Enforced via EFT's ToS or Privacy Policy",
      "transparentInformation": "Communicated via EFT's ToS or Privacy Policy",
      "directCollection": "Communicated via EFT's ToS or Privacy Policy",
      "indirectCollection": "Communicated via EFT's ToS or Privacy Policy",
      "rightOfAccess": "Exercised via EFT's web client",
      "rightToRectify": "Exercised via EFT's web client",
      "rightToBeForgotten": "Exercised via EFT's web client",
      "rightToRestrict": "Exercised via EFT's web client",
      "rightToBeNotified": "Exercised via EFT's event rules",
      "rightToExport": "Exercised via EFT's web client",
      "rightToObject": "Exercised via EFT's web client",
      "encryption": "Personal data is encrypted by EFT",
      "limitedAccess": "Configured By EFT",
      "purpose": {
        "type": "Configured By EFT",
        "reason": ""
      },
      "necessity": {
        "type": "Configured By EFT",
        "reason": ""
      },
      "riskAssessment": "EFT generated DPIA report",
      "riskMitigation": {
        "type": "Configured By EFT",
        "reason": ""
      },
      "dpoAssigned": {
        "type": "Configured By EFT",
        "email": "pofficer@mail.com"
      },
      "transferSafeguard": "Configured By EFT"
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).


```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "gdpr", "attributes":
{ "materialScope": "In scope",

"territorialScope": { "type": "In Union, all subjects in scope (3.1)", "value": {
"showEUStatus": true,

"allUsersToChangeEUSubject": true } }, "processingPrinciples": "General guidance not yet
met",

"lawfulnessOfProcessing": "Data subject consent (6.1.a)", "conditionsForConsent": "Set
via EFT's ToS or Privacy Policy",

"ageRestrictions": "Enforced via EFT's ToS or Privacy Policy", "transparentInformation":

"Communicated via EFT's ToS or Privacy Policy", "directCollection": "Communicated via
EFT's ToS or Privacy Policy",

"indirectCollection": "Communicated via EFT's ToS or Privacy Policy", "rightOfAccess":
"Exercised via EFT's web client",

"rightToRectify": "Exercised via EFT's web client", "rightToBeForgotten": "Exercised via
EFT's web client",

"rightToRestrict": "Exercised via EFT's web client", "rightToBeNotified": "Exercised via
EFT's event rules",

"rightToExport": "Exercised via EFT's web client", "rightToObject": "Exercised via EFT's
web client", "encryption":

"Personal data is encrypted by EFT", "limitedAccess": "Configured By EFT", "purpose": {
"type": "Configured By EFT",

"reason": "" }, "necessity": { "type": "Configured By EFT", "reason": "" },
"riskAssessment": "EFT generated DPIA report",

"riskMitigation": { "type": "Configured By EFT", "reason": "" }, "dpoAssigned": {
"type":

"Configured By EFT", "email": "" }, "transferSafeguard": "Configured By EFT" } },
"links": {

"self": "/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/gdpr" } }
```


PATCH PowerShell Sample

```
### PATCH GDRP Settings###

### User must obtain the SiteID from Get Sites

Write-Output "PATCH GDRP Settings"

Write-Output "--------------------"

$update =

'{
```

```
"data": {
  "type": "gdpr",
  "attributes": {
    "materialScope": "In scope",
    "territorialScope": {
      "type": "In Union, all subjects in scope (3.1)",
      "value": {
        "showEUStatus": true,
        "allUsersToChangeEUSubject": true
      }
    },
    "processingPrinciples": "General guidance not yet met",
    "lawfulnessOfProcessing": "Data subject consent (6.1.a)",
    "conditionsForConsent": "Set via EFT\u0027s ToS or Privacy Policy",
    "ageRestrictions": "Enforced via EFT\u0027s ToS or Privacy Policy",
    "transparentInformation": "Communicated via EFT\u0027s ToS or Privacy Policy",
    "directCollection": "Communicated via EFT\u0027s ToS or Privacy Policy",
    "indirectCollection": "Communicated via EFT\u0027s ToS or Privacy Policy",
    "rightOfAccess": "Exercised via EFT\u0027s web client",
    "rightToRectify": "Exercised via EFT\u0027s web client",
    "rightToBeForgotten": "Exercised via EFT\u0027s web client",
    "rightToRestrict": "Exercised via EFT\u0027s web client",
    "rightToBeNotified": "Exercised via EFT\u0027s event rules",
    "rightToExport": "Exercised via EFT\u0027s web client",
    "rightToObject": "Exercised via EFT\u0027s web client",
    "encryption": "Personal data is encrypted by EFT",
    "limitedAccess": "Configured By EFT",
    "purpose": {
      "type": "Configured By EFT",
      "reason": ""
    },
    "necessity": {
      "type": "Configured By EFT",
      "reason": ""
    },
    "riskAssessment": "EFT generated DPIA report",
    "riskMitigation": {
```

```
        "type": "Configured By EFT",
        "reason": ""
      },
      "dpoAssigned": {
        "type": "Configured By EFT",
        "email": "pofficer@mail.com"
      },
      "transferSafeguard": "Configured By EFT"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/gdpr"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/uploadForms

Returns and updates the upload forms configuration for specific profile

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/uploadForms
```

GET Body Sample

```
### GET the Upload Forms Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/uploadForms/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": [ { "type": "site", "id": "0de7387f-1506-427d-b997-e18bcdb8cbae",
"attributes": { "name": "MySite1" }, "links": { "self":
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae", "metrics":
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/metrics" } } ],
"links": { "self": "admin/v2/sites" } }
```

GET PowerShell Sample

```
###GET Upload Forms Settings###
Write-Output "GET Upload Forms Settings"
Write-Output "-----------------"
#$siteID = "Enter site ID"
$UpFormslist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/uploadForms"
-Method 'GET' -Headers $authHeader
Write-Output $UpFormslist | ConvertTo-Json -Depth 25
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/{siteId}/
```

POST Body Sample

```
###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/uploadForms/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "uploadFormName",
    "attributes": {
      "description": "Testing Forms from POST REST API",
      "displayName": "FORM_1",
      "displayInstruction": "Enter Text",
      "enabled": true,
      "showForEachFileUploaded": true,
      "userGroupId": "A0DB9377-92A3-4A38-8C0F-09F268D78FF1",
      "uploadFormElements": [
        {
          "name": "",
          "displayLabel": "FORM_1",
          "type": "string",
          "values": "domain.com",
          "required": true
        }
      ]
    }
  }
}
```

POST Response Body Sample

```
{"data":{"type":"uploadForm","id":"uploadFormName","attributes":{"id":"uploadFormName",
"type":"uploadForm","attributes":{"description":"Testing Forms from POST REST API",
"displayName":"FORM_1","displayInstruction":"Enter Text","enabled":true,
```

```
"showForEachFileUploaded":true,"userGroupId":"a0db9377-92a3-4a38-8c0f-09f268d78ff1",
"uploadFormElements":[{"name":"","displayLabel":"FORM_
1","type":"String","values":"domain.com",
"required":true}]}}},"links":{"self":"/admin/v2/sites/6203305a-d7c6-499e-a59b-
81500765f8f2/uploadForm/uploadFormName",
"userGroups":"/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/userGroups"}}
```


POST PowerShell Sample

```
$update =
'{
  "data": {
    "id": "uploadFormName",
    "attributes": {
      "description": "Testing Forms from POST REST API",
      "displayName": "FORM_once",
      "displayInstruction": "Enter Text",
      "enabled": true,
      "showForEachFileUploaded": true,
      "userGroupId": "A0DB9377-92A3-4A38-8C0F-09F268D78FF1",
      "uploadFormElements": [
        {
          "name": "",
          "displayLabel": "FORM_once",
          "type": "string",
          "values": "domain.com",
          "required": true
        }
      ]
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$postUploadFormsReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/uploadForms"
-Method 'POST' -Headers $authHeader -Body $update
Write-Output $postUploadFormsReturn | ConvertTo-Json
```

Endpoint: /sites/{siteId}/uploadForms/{uploadFormName}

Returns site upload settings. Update site upload forms settings. Deletes upload form.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/uploadForms/{uploadFormName}
```

GET Body Sample

```
### GET Specific Upload Forms Settings####
### Enter the form ID


@upLoadFormsID = {{formsList.response.body.$.data[0].id}}


GET https://{{host}}/admin/v2/sites/{{Siteid}}/uploadForms/{{upLoadFormsID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{"data":{"id":"uploadFormName","type":"uploadForm","attributes":{"description":"Testing
Forms from POST REST API",
"displayName":"FORM_1","displayInstruction":"Enter
Text","enabled":true,"showForEachFileUploaded":true,
"userGroupId":"a0db9377-92a3-4a38-8c0f-09f268d78ff1","uploadFormElements":
[{"name":"","displayLabel":"FORM_1",
"type":"String","values":"domain.com","required":true}]}},"links":{"self":
"/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/uploadForm/uploadFormName",
"userGroups":"/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/userGroups"}}
```

GET PowerShell Sample

```
###GET Upload Forms Settings###
Write-Output "GET Upload Forms Settings"
Write-Output "-----------------"
#$siteID = "Enter site ID"
$UpFormslist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/uploadForms"
-Method 'GET' -Headers $authHeader
Write-Output $UpFormslist | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH  https://[server URL]:[port]/admin/v2/sites/
{siteId}/uploadForms/{uploadFormName}
```

PATCH Body Sample

```
###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/uploadForms/{{upLoadFormsID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "uploadFormName",
    "type": "uploadForm",
    "attributes": {
      "description": "Testing Forms from POST REST API",
      "displayName": "FORM_1",
      "displayInstruction": "Enter Text",
      "enabled": true,
      "showForEachFileUploaded": false,
      "userGroupId": "a0db9377-92a3-4a38-8c0f-09f268d78ff1",
      "uploadFormElements": [
        {
          "name": "",
          "displayLabel": "FORM_1",
          "type": "String",
          "values": "domain.com",
```

```
          "required": true
        }
      ]
    }
  }
}
```

POST Response Body Sample

```
{"data":{"id":"uploadFormName","type":"uploadForm","attributes":{"description":"Testing
Forms from POST REST API",
"displayName":"FORM_1","displayInstruction":"Enter
Text","enabled":true,"showForEachFileUploaded":false,
"userGroupId":"a0db9377-92a3-4a38-8c0f-09f268d78ff1","uploadFormElements":
[{"name":"","displayLabel":"FORM_1",
"type":"String","values":"domain.com","required":true}]}},"links":{"self":
"/admin/v2/sites/6203305a-d7c6-499e-a59b-
81500765f8f2/uploadForms/uploadFormName","userGroups":
"/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/userGroups"}}
```

PATCH PowerShell Sample

```
$update =
'{
  "data": {
    "id": "uploadFormName",
    "type": "uploadForm",
    "attributes": {
      "description": "Testing Forms from POST REST API",
      "displayName": "FORM_1",
      "displayInstruction": "Enter New Text",
      "enabled": true,
      "showForEachFileUploaded": false,
      "userGroupId": "a0db9377-92a3-4a38-8c0f-09f268d78ff1",
      "uploadFormElements": [
        {
          "name": "",
          "displayLabel": "FORM_1",
```

```
          "type": "String",
          "values": "domain.com",
          "required": true
        }
      ]
    }
  }
}
'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchUploadFormsReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/uploadForms/$formsID"
-Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $patchUploadFormsReturn | ConvertTo-Json
```

DELETE Body Sample

```
### GET Specific Upload Forms Settings####
### Enter the form ID

@upLoadFormsID = {{formsList.response.body.$.data[0].id}}

DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/uploadForms/{{upLoadFormsID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content
Date: Mon, 08 Aug 2022 20:43:09 GMT
Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate
Expires: -1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
```

```
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
$formsID = $uploadFList.data[0].id


$deleteUploadFList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/uploadForms/$formsID"
-Method 'DELETE' -Headers $authHeader
Write-Output $deleteUploadFList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/outlookDeploymentScript

Returns the outlook deployment script.

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/outlookDeploymentScript
```

GET Body Sample

```
## GET outlook Deployment Script####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/outlookDeploymentScript HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
msiexec /lv installation.log /qn /i EFTOutlookAddinInstaller.msi
EFTHOST=http://172.31.223.227 EFTPORT=443 EFTAUTHTYPE=MANUAL
EFTUSERNAME=username EFTPASSWORD=test123!
INSTALLLOCATION="%userprofile%\AppData\Roaming\GlobalSCAPE\EFT Outlook Add-in"
FILESTORELOCATION="%userprofile%\AppData\Local\GlobalSCAPE\EFT Outlook Add-in"
```

GET PowerShell Sample

```
###GET outlook Deployment Script###
Write-Output "GET outlook Deployment Script"
Write-Output "-----------------"
#$siteID = "Enter site ID"
$ODSlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/outlookDeploymentScript"
-Method 'GET' -Headers $authHeader
Write-Output $ODSlist | ConvertTo-Json -Depth 25
```

Endpoint: /sites/{siteId}/contentIntegrity

Returns and updates the content integrity settings for specific site.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/contentIntegrity
```

GET Body Sample

```
### GET a list of current content integrity profiles####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": [ { "id": "6f61c6c0-221e-4f01-94d0-46ba78ec0548", "type": "contentIntegrity",
"attributes": { "profileName": "TEST API" } }, { "id": "03bebeda-1a89-40d2-a8c8-
78ec078257db",
"type": "contentIntegrity", "attributes": { "profileName": "TEST API 2" } } ], "links":
{
"self": "admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/contentIntegrity" } }
```

GET PowerShell Sample

```
###GET list of Content Integrity Profiles###
Write-Output "GET list of Content Integrity Profiles"
Write-Output "-------------------------------------"
#$siteID = "Enter site ID"
$CIlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/contentIntegrity"
-Method 'GET' -Headers $authHeader
Write-Output $CIlist | ConvertTo-Json -Depth 25
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/
{siteId}/contentIntegrity
```

POST Body Sample

```
### #POST content integrity profile ####
POST https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
  "data": {
    "type": "contentIntegrity",
    "attributes": {
      "profileName": "Profile_API_TEST5",
      "host": "192.168.100.82",
      "port": 1344,
      "path": "/reqmode",
      "mode": "REQMOD",
      "scanLimit": {
        "enabled": true,
        "bytes": 100000
      },
      "headerOverrides": {
        "httpHost": {
          "enabled": true,
          "value": "192.168.100.83"
        },
        "xClientIp": {
          "enabled": true,
          "value": "192.168.100.52"
        },
        "xServerIp": {
          "enabled": true,
          "value": "192.168.100.60"
        },
        "xSubscriberIp": {
          "enabled": true,
```

```
          "value": "192.168.100.70"
        },
        "xAuthenticatedUser": {
          "enabled": true,
          "value": "192.186.100.12"
        },
        "xAuthenticatedGroups": {
          "enabled": true,
          "value": "Local://%USER.Log%"
        }
      },
      "responseHandling": {
        "continueOnConnectivityError": "Continue",
        "continueOnHttpError": "Continue",
        "continueOnIcapViolation": "Fail",
        "continueOnIcapRedaction": "Continue",
        "customHeadersToAudit": {
          "enabled": true,
          "headers": []
        }
      }
    }
  }
}
```


POST Response Body Sample


```
{ "data": { "id": "53f00be5-9aa0-41ed-9fdf-ea99f6784238", "type": "contentIntegrity",
"attributes": { "profileName": "Profile_API_TEST", "host": true, "port": 1344, "path":
true,
"mode": "REQMOD", "scanLimit": { "enabled": true, "bytes": 100000 }, "headerOverrides":
{ "httpHost": {
"enabled": true, "value": "192.168.100.83" }, "xClientIp": { "enabled": true, "value":
"192.168.100.52" },
"xServerIp": { "enabled": false, "value": "" }, "xSubscriberIp": { "enabled": false,
"value": "" },
"xAuthenticatedUser": { "enabled": false, "value": "" }, "xAuthenticatedGroups": {
"enabled": false,
"value": "" } }, "responseHandling": { "continueOnConnectivityError": "Continue",
```

```
"continueOnHttpError": "Continue", "continueOnIcapViolation": "Fail",
"continueOnIcapRedaction": "Continue",
"customHeadersToAudit": { "enabled": true, "headers": [] } } } }, "links": {
"self": "admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/contentIntegrity/
53f00be5-9aa0-41ed-9fdf-ea99f6784238" } }
```

POST PowerShell Sample

```
###POST Create New Content Integrity Profile###
Write-Output " Create New Content Integrity Profile"
Write-Output "-------------------------------------"
$update =
'{
  "data": {
    "type": "contentIntegrity",
    "attributes": {
      "profileName": "Profile_API_TEST6",
      "host": "192.168.100.82",
      "port": 1344,
      "path": "/reqmode",
      "mode": "REQMOD",
      "scanLimit": {
        "enabled": true,
        "bytes": 100000
      },
      "headerOverrides": {
        "httpHost": {
          "enabled": true,
          "value": "192.168.100.83"
        },
        "xClientIp": {
          "enabled": true,
          "value": "192.168.100.52"
        },
        "xServerIp": {
          "enabled": true,
          "value": "192.168.100.60"
```

```
        },
        "xSubscriberIp": {
          "enabled": true,
          "value": "192.168.100.70"
        },
        "xAuthenticatedUser": {
          "enabled": true,
          "value": "192.186.100.12"
        },
        "xAuthenticatedGroups": {
          "enabled": true,
          "value": "Local://%USER.Log%"
        }
      },
      "responseHandling": {
        "continueOnConnectivityError": "Continue",
        "continueOnHttpError": "Continue",
        "continueOnIcapViolation": "Fail",
        "continueOnIcapRedaction": "Continue",
        "customHeadersToAudit": {
          "enabled": true,
          "headers": []
        }
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 25
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/contentIntegrity"
-Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/contentIntegrity/{profileId}

Returns, updates, and deletes content integrity profile settings.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/contentIntegrity/{profileId}
```

GET Body Sample

```
### GET spacific content integrity profile settings####

###Pass the ID of the CIC profile###

@profileId = 53f00be5-9aa0-41ed-9fdf-ea99f6784238

GET https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity/{{profileId}}/ HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "id": "53f00be5-9aa0-41ed-9fdf-ea99f6784238", "type": "contentIntegrity",

"attributes": { "profileName": "Profile_API_TEST", "host": true, "port": 1344, "path":
true,

"mode": "REQMOD", "scanLimit": { "enabled": true, "bytes": 100000 },

"headerOverrides": { "httpHost": { "enabled": true, "value": "192.168.100.83" },

"xClientIp": { "enabled": true, "value": "192.168.100.52" }, "xServerIp": { "enabled":
false, "value": "" },

"xSubscriberIp": { "enabled": false, "value": "" }, "xAuthenticatedUser": { "enabled":
false, "value": "" },

"xAuthenticatedGroups": { "enabled": false, "value": "" } },

"responseHandling": { "continueOnConnectivityError": "Continue", "continueOnHttpError":
"Continue",

"continueOnIcapViolation": "Fail", "continueOnIcapRedaction": "Continue",

"customHeadersToAudit": { "enabled": true, "headers": [] } } } }, "links": { "self":

"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/contentIntegrity/53f00be5-9aa0-
41ed-9fdf-ea99f6784238" } }
```

GET PowerShell Sample

```
####Added 2/15/2022 ###

###GET specific Content Integrity Profile settings###

### User must obtain the Profile ID and manually enter it or by holding the value on a
variable ###

Write-Output "GET specific Content Integrity Profile settings"

Write-Output "--------------------------------------------"

#$profileID = "53f00be5-9aa0-41ed-9fdf-ea99f6784238"

$SCIlist = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/contentIntegrity/$profileId"

-Method 'GET' -Headers $authHeader

Write-Output $SCIlist | ConvertTo-Json -Depth 35
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/contentIntegrity/{profileId}
```

PATCH Body Sample

```
### #PATCH content integrity profile ####

###Pass the ID of the CIC profile###

###@profileId = 53f00be5-9aa0-41ed-9fdf-ea99f6784238

PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity/{{profileId}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "contentIntegrity",
    "attributes": {
      "profileName": "Profile_API_TEST_PATCH",
      "host": true,
      "port": 1344,
      "path": true,
      "mode": "REQMOD",
      "scanLimit": {
        "enabled": true,
        "bytes": 100000
      },
```

```
    "headerOverrides": {
      "httpHost": {
        "enabled": true,
        "value": "192.168.100.00"
      },
      "xClientIp": {
        "enabled": true,
        "value": "192.168.100.00"
      },
      "xServerIp": {
        "enabled": false,
        "value": ""
      },
      "xSubscriberIp": {
        "enabled": false,
        "value": ""
      },
      "xAuthenticatedUser": {
        "enabled": false,
        "value": ""
      },
      "xAuthenticatedGroups": {
        "enabled": false,
        "value": ""
      }
    },
    "responseHandling": {
      "continueOnConnectivityError": "Continue",
      "continueOnHttpError": "Continue",
      "continueOnIcapViolation": "Fail",
      "continueOnIcapRedaction": "Continue",
      "customHeadersToAudit": {
        "enabled": true,
        "headers": []
      }
    }
  }
```

```
  }
}
```

PATCH Response Body Sample

```
{ "data": { "id": "d7c7c566-e2e1-4dd9-8332-9c2aa63f7bff", "type": "contentIntegrity",
"attributes": { "profileName": "Profile_API_TEST_PATCH", "host": true, "port": 1344,
"path": true,
"mode": "REQMOD", "scanLimit": { "enabled": true, "bytes": 100000 },
"headerOverrides": { "httpHost": { "enabled": true, "value": "192.168.100.00" },
"xClientIp": { "enabled": true, "value": "192.168.100.00" }, "xServerIp": { "enabled":
false,
"value": "" }, "xSubscriberIp": { "enabled": false, "value": "" }, "xAuthenticatedUser":
{
"enabled": false, "value": "" }, "xAuthenticatedGroups": { "enabled": false, "value": ""
} },
"responseHandling": { "continueOnConnectivityError": "Continue", "continueOnHttpError":
"Continue",
"continueOnIcapViolation": "Fail", "continueOnIcapRedaction": "Continue",
"customHeadersToAudit": { "enabled": true, "headers": [] } } } }, "links": { "self":
"/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/contentIntegrity/d7c7c566-e2e1-
4dd9-8332-9c2aa63f7bff" } }
```

PATCH PowerShell Sample

```
### PATCH specific Content Integrity Profile settings###
### User must obtain the Profile ID and manually enter it or by holding the value on a
variable ###
Write-Output "PATCH specific Content Integrity Profile settings"
Write-Output "-----------------------------------------------"
$update =
'{
  "data": {
    "type": "contentIntegrity",
    "attributes": {
      "profileName": "Profile_API_TEST_PATCH",
      "host": true,
      "port": 1344,
      "path": true,
      "mode": "REQMOD",
```

```
  "scanLimit": {
    "enabled": true,
    "bytes": 100000
  },
  "headerOverrides": {
    "httpHost": {
      "enabled": true,
      "value": "192.168.100.00"
    },
    "xClientIp": {
      "enabled": true,
      "value": "192.168.100.00"
    },
    "xServerIp": {
      "enabled": false,
      "value": ""
    },
    "xSubscriberIp": {
      "enabled": false,
      "value": ""
    },
    "xAuthenticatedUser": {
      "enabled": false,
      "value": ""
    },
    "xAuthenticatedGroups": {
      "enabled": false,
      "value": ""
    }
  },
  "responseHandling": {
    "continueOnConnectivityError": "Continue",
    "continueOnHttpError": "Continue",
    "continueOnIcapViolation": "Fail",
    "continueOnIcapRedaction": "Continue",
    "customHeadersToAudit": {
      "enabled": true,
```

```
          "headers": []
        }
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 35
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/contentIntegrity/$profileId"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/
{siteId}/contentIntegrity/{profileId}
```

DELETE Body Sample

```
###DELETE spacific content integrity profile settings####
###Pass the ID of the CIC profile###
###@profileId = 53f00be5-9aa0-41ed-9fdf-ea99f6784238
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity/{{profileId}}/
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
###DELETE spacific content integrity profile settings####
###Pass the ID of the CIC profile###
###@profileId = 53f00be5-9aa0-41ed-9fdf-ea99f6784238
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity/{{profileId}}/
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE PowerShell Sample

```
###DELETE specific content integrity profile settings####
```

```
###Pass the ID of the CIC profile###

###@profileId = 53f00be5-9aa0-41ed-9fdf-ea99f6784238

Write-Output "DELETE specific content integrity profile settings"

Write-Output "-------------------------------------------------"

#$profileID = "53f00be5-9aa0-41ed-9fdf-ea99f6784238"

$DCIClist = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/contentIntegrity/$profileId"

-Method 'DELETE' -Headers $authHeader

Write-Output $DCIClist | ConvertTo-Json -Depth 35
```

Endpoint: /sites/{siteId}/custom-commands

Note: Available as of EFT 8.1.0

This endpoint provides the ability to return a list of custom commands defined on an EFT site or create a new custom command.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/custom-commands
```

GET Body Sample

```
###
##Get Site Custom Commands
GET https://{{host}}/admin/v2//sites/{{siteId}}/custom-commands HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": [ { "id": "9a0c4aec-862e-4e72-aec4-9b1f04f00bb3", "type": "customCommand",
"attributes": { "name": "Command 1" },
"links": { "self": "/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/
custom-commands/9a0c4aec-862e-4e72-aec4-9b1f04f00bb3" } },
{ "id": "090dde3a-c039-44ab-b03d-5cc994548ce7", "type":
"customCommand", "attributes": { "name": "Run to the Moon" },
"links": { "self": "/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/custom-
commands/
090dde3a-c039-44ab-b03d-5cc994548ce7" } } ],
"links": { "self": "/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/custom-
commands" } }
```

GET PowerShell Sample

```
###
#Get Site Custom Commands
Write-Output "Get Site Custom Commands"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-commands"
-Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Method & URL

`POST https://[server URL]:[port]/admin/v2/sites/{siteId}/custom-commands`

POST Body Sample

```
## Create Custom Command on a specific EFT Site
POST https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data":{
        "id":"",
        "type": "customCommand",
            "attributes": {
                "enabled": true,
                "name": "Command 5",
                "description": "this is a test to run command 5",
                "executable": "c:\\windows\\system32\\cscript.exe \
                "c:\\users\\administrator\\desktop\\server.vbs\"",
                "parameters": "",
                "redirectOutputToLog": true,
                "useProcessTimeOut": true,
                "processTimeOut": 30,
                "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log",
                "redirectOutputToClient": true,
```

```
                "useMinNumOfParams": false,
                "minNumOfParams": 1,
                "minNumOfParamsMsg": ""
            }
    }
}
###
```

POST Response Body Sample

```
{ "data": { "id": "f1d88549-e4aa-49da-b685-536fe0d93b62", "type": "customCommand",
"attributes": { "enabled": true,
"name": "Command 5", "description": "this is a test to run command 5",
"executable": "c:\\windows\\system32\\cscript.exe
\"c:\\users\\administrator\\desktop\\server.vbs\"",
"parameters": "", "redirectOutputToLog": true, "useProcessTimeOut": true,
"processTimeOut": 30,
"logFileName": "C:\\ProgramData\\Globalscape\\EFT Server\\Logs\\cmdout.log",
"redirectOutputToClient": true, "useMinNumOfParams": false, "minNumOfParams": 1,
"minNumOfParamsMsg": "" },
"relationships": { "executionPermissions": { "data": { "users": [], "userGroups": [ {
"type": "userGroup", "id": "a0db9377-92a3-4a38-8c0f-09f268d78ff1", "meta": { "name":
"All Users" } } ] } } },
"links": { "self": "/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/custom-
commands/
f1d88549-e4aa-49da-b685-536fe0d93b62" } } }
```

POST PowerShell Sample

```
###
#POST new site Custom Command
Write-Output "POST Custom Command (New Custom Command)"
Write-Output "-----"
$update =
'{
    "data":{
        "id":"",
        "type": "customCommand",
            "attributes": {
```

```
                "enabled": true,
                "name": "Command 5",
                "description": "this is a test to run command 5",
                "executable": "c:\\windows\\system32\\cscript.exe
\"c:\\users\\administrator\\desktop\\server.vbs\"",
                "parameters": "",
                "redirectOutputToLog": true,
                "useProcessTimeOut": true,
                "processTimeOut": 30,
                "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log",
                "redirectOutputToClient": true,
                "useMinNumOfParams": false,
                "minNumOfParams": 1,
                "minNumOfParamsMsg": ""
            }
    }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-commands"
-Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/custom-commands/{customCommandID}

Note: Available as of EFT 8.1.0

Returns a custom command defined on an EFT site and allows the ability to get, patch (update), and delete the custom command.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/custom-commands/{customCommandID}
```

GET Body Sample

```
### Get Custom Commands for a Site ###

# @name customCommandList

GET https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###

@customCommandID = {{customCommandList.response.body.$.data[0].id}}


### Get specific Custom Command from a Site ###

GET https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands/{{customCommandID}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample

```
{ "data": { "id": "9a0c4aec-862e-4e72-aec4-9b1f04f00bb3", "type": "customCommand", "attributes": {

"enabled": true, "name": "Command 1", "description": "this is a test to run command 1", "executable":
```

```
"c:\\windows\\system32\\cscript.exe \"c:\\users\\administrator\\desktop\\server.vbs\"",
"parameters": "",

"redirectOutputToLog": true, "useProcessTimeOut": true, "processTimeOut": 30,
"logFileName":

"C:\\ProgramData\\Globalscape\\EFT Server\\Logs\\cmdout.log", "redirectOutputToClient":
true,

"useMinNumOfParams": false, "minNumOfParams": 1, "minNumOfParamsMsg": "" },
"relationships": {

"executionPermissions": { "data": { "users": [], "userGroups": [ { "type": "userGroup",
"id":

"a0db9377-92a3-4a38-8c0f-09f268d78ff1", "meta": { "name": "All Users" } } ] } } },
"links": {

"self": "/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/custom-commands/

9a0c4aec-862e-4e72-aec4-9b1f04f00bb3" } } }
```

GET PowerShell Sample

```
###

#Get Site Custom Commands

Write-Output "Get Site Custom Commands"

Write-Output "-----"

$commands = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-commands"

-Method 'GET' -Headers $authHeader

#Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10

foreach ($commands in $commands.id)

{

    Write-Output ("Custom Command found:  $($commands.id):
$($commands.attributes.name)")

}

$customCommandID = $commands.data[0].id


###

#Get Custom Command

Write-Output "Get Custom Commands for: "  $customCommandID

Write-Output "-----"

$commandList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-
commands/$customCommandID"

-Method 'GET' -Headers $authHeader

Write-Output $commandList | ConvertTo-Json -Depth 10
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/custom-commands/{customCommandID}
```

PATCH Body Sample

```
### Get Custom Commands for a Site which is needed to patch a Custom Commmand ###

# @name customCommandList

GET https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###

@customCommandID = {{customCommandList.response.body.$.data[0].id}}


###

#Path Custom Command on a specific EFT site

PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands/{{customCommandID}}
HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}


{
    "data":{
        "id":"",
        "type": "customCommand",
            "attributes": {
                "enabled": true,
                "name": "Updated Custom Command Name",
                "description": "Updated Custom Command Description",
                "executable": "c:\\windows\\system32\\cscript.exe
\"c:\\users\\administrator\\desktop\\server.vbs\"",
                "parameters": "",
                "redirectOutputToLog": true,
                "useProcessTimeOut": false,
                "processTimeOut": 30,
                "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log",
                "redirectOutputToClient": true,
                "useMinNumOfParams": false,
                "minNumOfParams": 1,
                "minNumOfParamsMsg": ""
```

```
            }
    }
}
###
```

PATCH Response Body Sample

```
{ "data": { "id": "9a0c4aec-862e-4e72-aec4-9b1f04f00bb3", "type": "customCommand",
"attributes": { "enabled": true, "name": "Updated Custom Command Name", "description":
"Updated Custom Command Description", "executable": "c:\\windows\\system32\\cscript.exe
\
"c:\\users\\administrator\\desktop\\server.vbs\"", "parameters": "",
"redirectOutputToLog": true, "useProcessTimeOut": false, "processTimeOut": 30,
"logFileName": "C:\\ProgramData\\Globalscape\\EFT Server\\Logs\\cmdout.log",
"redirectOutputToClient": true, "useMinNumOfParams": false, "minNumOfParams": 1,
"minNumOfParamsMsg": "" }, "relationships": { "executionPermissions": { "data": {
"users": [], "userGroups": [ { "type": "userGroup", "id": "a0db9377-92a3-4a38-8c0f-
09f268d78ff1",
"meta": { "name": "All Users" } } ] } } }, "links": { "self": "/admin/v2/sites/
c7d3ecfe-a100-4bcd-b830-01a10524c048/custom-commands/9a0c4aec-862e-4e72-aec4-
9b1f04f00bb3" } } }
```

PATCH PowerShell Sample

```
############################
#Patch a Custom Command
###
#Get Site Custom Commands
Write-Output "Get Site Custom Commands in order to Patch"
Write-Output "-----"
$commands = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-commands" -Method
'GET' -Headers $authHeader
#Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($commands in $commands.id)
{
    Write-Output ("Custom Command found:  $($commands.id):
$($commands.attributes.name)")
}
```

```
$customCommandID = $commands.data[0].id


#PATCH Custom Command
Write-Output "Custom Command Patch"
Write-Output "Custom Command: $customCommandID"
Write-Output "-----"
$update =
'{
    "data":{
        "id":"",
        "type": "customCommand",
            "attributes": {
                "enabled": true,
                "name": "Updated Custom Command Name 2",
                "description": "Updated Custom Command Description 2",
                "executable": "c:\\windows\\system32\\cscript.exe \
                "c:\\users\\administrator\\desktop\\server.vbs\"",
                "parameters": "",
                "redirectOutputToLog": true,
                "useProcessTimeOut": false,
                "processTimeOut": 30,
                "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log",
                "redirectOutputToClient": true,
                "useMinNumOfParams": false,
                "minNumOfParams": 1,
                "minNumOfParamsMsg": ""
            }
    }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-
commands/$customCommandID"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/
{siteId}/custom-commands/{customCommandID}
```

DELETE Body Sample

```
##DELETE Custom Commands

### Get Custom Commands for a Site which is needed to delete a Custom Commmand ###

# @name customCommandList

GET https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###

@customCommandID = {{customCommandList.response.body.$.data[0].id}}

#


##Delete Request passing custom command id

DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands/{{customCommandID}}
HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Fri, 15 Jul 2022 21:48:08 GMT Content-Length: 0 Cache-
Control: no-cache,

no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection:
1;

mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;

Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
### DELETE CUSTOM COMMAND

#Get Site Custom Commands in order to get custom command id

Write-Output "Get Site Custom Commands in order to Delete"

Write-Output "-----"

$commands = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-commands" -Method
'GET'
```

```
-Headers $authHeader

#Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10

foreach ($commands in $commands.id)

{

    Write-Output ("Custom Command found:  $($commands.id):
$($commands.attributes.name)")

}

$customCommandID = $commands.data[0].id


Write-Output "Deleting Custom Command: "  $customCommandID

Write-Output "-----"

$commandList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-
commands/$customCommandID"

-Method 'DELETE' -Headers $authHeader

Write-Output $commandList | ConvertTo-Json -Depth 10
```

Endpoint: /sites/{siteId}/user-templates

Note: Available as of EFT 8.1.0

Returns a list of user templates defined on an EFT site and allows the ability to get and create templates.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/user-templates
```

GET Body Sample

```
### Get User Settings Template ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{ "data": [ { "attributes": { "as2": { "inbound": { "enabled": true }, "outbound": {
"enabled": true } },
"changePassword": { "enabled": "inherit", "value": {
"changeAdminProvidedPasswordUponFirstUse": "inherit",
"passwordExpiration": { "enabled": true, "value": { "maxAgeDays": 90, "emailUpon": true,
"remindPrior": {
"enabled": false, "value": { "daysBefore": 5, "emailUser": true } } } } } },
"connectionTimeout": {
"enabled": true, "value": { "maxSec": 600 } }, "connectionsFromSameIpLimit": {
"enabled": false,
"value": { "maxNumber": 0 } }, "downloadSizeLimit": { "enabled": false, "value": {
"maxKBytes": 0 } },
"downloadsPerSessionLimit": { "enabled": false, "value": { "maxNumber": 0 } },
"enabled": true,
"ftp": { "enabled": true, "value": { "enableFxp": "inherit", "enableNoop": "inherit",
"enableComb": "yes", "enableXcrc": "yes", "enableZlib": true, "banner": { "message":
"Login OK. Proceed.",
```

```
"usage": "replaceDefault" } } }, "ftps": { "enabled": true }, "hasHomeFolderAsRoot":
true, "homeFolder": {

"enabled": true, "value": { "path": "/" } }, "http": { "enableHttp": true,
"enableHttps": true,

"enableWtc": true, "enableShareFolder": true, "enableSendMessage": true },
"invalidLoginLimit": {

"enabled": "inherit", "value": { "maxCount": 90, "periodMin": 5, "action": "lock",
"actionDurationMin": 30 } },

"ipAccessLimit": { "enabled": false, "value": { "rules": [], "defaultRule":
"allowAccess" } }, "name":

"Default Settings", "passwordComplexity": { "enabled": "inherit", "value": {
"minLength": 8,

...

"definedUserTemplates": 4 } }
```


GET PowerShell Sample

```
# get sites

Write-Output "Site"

Write-Output "----"

$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites"

-Method 'GET' -Headers $authHeader

Write-Output $siteList | ConvertTo-Json

foreach ($site in $siteList.data)

{

    Write-Output ("Site  $($site.id): $($site.attributes.name)")

}


$siteID = $siteList.data[0].id


###

#Get Site User Settings Template

Write-Output "Get Site User Settings Template"

Write-Output "-----"

$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-templates"

-Method 'GET' -Headers $authHeader

Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10

##
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/{siteId}/user-templates
```

POST Body Sample

```
### POST User Settings Template (Create)###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data":{
        "type": "userTemplate",
        "attributes":{
            "name": "GSB Template 4",
            "accountEnabled": true,
            "homeFolder": {
                "enabled": false,
                "value": {
                    "path": ""
                }
            }
        },
        "passwordComplexity": {
          "enabled": "inherit",
          "value": {
            "minLength": 8,
            "characterCategories": {
              "enabled": true,
              "value": {
                "characterCount": 4,
                "upperCaseRequired": true,
                "lowerCaseRequired": true,
                "numericRequired": true,
                "nonAlphaNumericRequired": false,
                "non7bitAsciiRequired": false
              }
```

```
      },
      "usernameCharLimit": {
        "enabled": true,
        "value": {
          "minDisallowed": 3
        }
      }
    }
  },
  "sftp": {
    "enabled": true,
    "value": {
      "authenticationType": "password"
    }
  },
  "ssl": {
    "authenticationType": "password"
  }     }}
```


POST Response Body Sample


```
{ "data": { "attributes": { "as2": { "inbound": { "enabled": true }, "outbound": {
"enabled": true } },

"changePassword": { "enabled": "inherit", "value": {
"changeAdminProvidedPasswordUponFirstUse": "inherit",

"passwordExpiration": { "enabled": true, "value": { "maxAgeDays": 90, "emailUpon": true,
"remindPrior": {

"enabled": false, "value": { "daysBefore": 5, "emailUser": true } } } } } },
"connectionTimeout": {

"enabled": true, "value": { "maxSec": 600 } }, "connectionsFromSameIpLimit": {

"enabled": false, "value": { "maxNumber": 0 } }, "downloadSizeLimit": {

"enabled": false, "value": { "maxKBytes": 0 } }, "downloadsPerSessionLimit": {

"enabled": false, "value": { "maxNumber": 0 } }, "enabled": true, "ftp": {

"enabled": true, "value": { "enableFxp": "inherit", "enableNoop": "inherit",

"enableComb": "yes", "enableXcrc": "yes", "enableZlib": true, "banner": { "message":
"Login OK. Proceed.",

"usage": "replaceDefault" } } }, "ftps": { "enabled": true }, "hasHomeFolderAsRoot":
true, "homeFolder": {

"enabled": false, "value": { "path": "/" } }, "http": { "enableHttp": true,
"enableHttps": true,
```

```
"enableWtc": true, "enableShareFolder": true, "enableSendMessage": true },
"invalidLoginLimit": {

"enabled": "inherit", "value": { "maxCount": 90, "periodMin": 5, "action": "lock",
"actionDurationMin": 30 } },

"ipAccessLimit": { "enabled": false, "value": { "rules": [], "defaultRule":
"allowAccess" } }, "name":

"GSB Template 4", "passwordComplexity": { "enabled": "inherit", "value": { "minLength":
8, "characterCategories": {

"enabled": true, "value": { "characterCount": 4, "upperCaseRequired": true,
"lowerCaseRequired": true,

"numericRequired": true, "nonAlphaNumericRequired": false, "non7bitAsciiRequired": false
} }, "usernameCharLimit": {

...

"type": "userTemplate" } }
```

POST PowerShell Sample

```
###

#POST Site User Settings Template (Create)

#POST new site Custom Command

Write-Output "POST User Settings Template (New User Settings Template)"

Write-Output "-----"

$update =

'{

    "data":{

        "type": "userTemplate",

        "attributes":{

            "name": "GSB Template 4",

            "accountEnabled": true,

            "homeFolder": {

                "enabled": false,

                "value": {

                    "path": ""

                }

            }

        },

        "passwordComplexity": {

          "enabled": "inherit",

          "value": {
```

```
            "minLength": 8,
            "characterCategories": {
              "enabled": true,
              "value": {
                "characterCount": 4,
                "upperCaseRequired": true,
                "lowerCaseRequired": true,
                "numericRequired": true,
                "nonAlphaNumericRequired": false,
                "non7bitAsciiRequired": false
              }
            },
            "usernameCharLimit": {
              "enabled": true,
              "value": {
                "minDisallowed": 3
              }
            }
          }
        },
        "sftp": {
          "enabled": true,
          "value": {
            "authenticationType": "password"
          }
        },
        "ssl": {
          "authenticationType": "password"
        }
      }

}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-templates"
-Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/user-templates/{userTemplateid}

Note: Available as of EFT 8.1.0

Returns a user settings template defined on an EFT site and allows the ability to get, update, and delete the user template.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/user-templates/{userTemplateid}
```

GET Body Sample

```
### Get User Settings Template ### Need to obtain templates first
# @name userTemplates
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@userTemplateid = {{userTemplates.response.body.$.data[3].id}}
#Update the array to obtain the desired user template


### GET User Template by Template ID ###
#
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates/{{userTemplateid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": { "attributes": { "as2": { "inbound": { "enabled": true }, "outbound": { "enabled": true } },
```

```
"changePassword": { "enabled": "inherit", "value": {
"changeAdminProvidedPasswordUponFirstUse": "inherit",

"passwordExpiration": { "enabled": true, "value": { "maxAgeDays": 90, "emailUpon": true,
"remindPrior": {

"enabled": false, "value": { "daysBefore": 5, "emailUser": true } } } } } },
"connectionTimeout": {

"enabled": true, "value": { "maxSec": 600 } }, "connectionsFromSameIpLimit": {
"enabled": false,

"value": { "maxNumber": 0 } }, "downloadSizeLimit": { "enabled": false, "value": {
"maxKBytes": 0 } },

"downloadsPerSessionLimit": { "enabled": false, "value": { "maxNumber": 0 } },
"enabled": false,

"ftp": { "enabled": true, "value": { "enableFxp": "inherit", "enableNoop": "inherit",
"enableComb": "yes",

"enableXcrc": "yes", "enableZlib": true, "banner": { "message": "Login OK. Proceed.",

"usage": "replaceDefault" } } }, "ftps": { "enabled": true }, "hasHomeFolderAsRoot":
true,

"homeFolder": { "enabled": true, "value": { "path": "/" } }, "http": { "enableHttp":
true,

"enableHttps": true, "enableWtc": true, "enableShareFolder": true, "enableSendMessage":
true },

"invalidLoginLimit": { "enabled": "inherit", "value": { "maxCount": 90, "periodMin": 5,

"action": "lock", "actionDurationMin": 30 } }, "ipAccessLimit": { "enabled": false,
"value": {

"rules": [], "defaultRule": "allowAccess" } }, "name": "GSB Template 2",
"passwordComplexity": {

"enabled": "inherit", "value": { "minLength": 8, "characterCategories": { "enabled":
true, "value": {

"characterCount": 4, "upperCaseRequired": true, "lowerCaseRequired": true,
"numericRequired": true,

"nonAlphaNumericRequired": false, "non7bitAsciiRequired": false } },
"usernameCharLimit": {

"enabled": true, "value": { "minDisallowed": 3 } }, "repeatingCharLimit": { "enabled":
true,

"value": { "minDisallowed": 3 } }, "forbiddenDictionary": { "enabled": true, "value": {
"dictionaryFilePath": "",

"noBackwardsWord": false } } } }, "passwordHistory": { "enabled": "inherit", "value": {
"historyDepth": 4 } },

"sftp": { "enabled": true, "value": { "authenticationType": "password" } }, "ssl": {

"authenticationType": "password" }, "totalConnectionsLimit": { "enabled": false,

"value": { "maxNumber": 0 } }, "transferSpeedLimit": { "enabled": false, "value": {

"maxKbps": 0 } }, "uploadSizeLimit": { "enabled": false, "value": { "maxKBytes": 0 } },

"uploadsPerSessionLimit": { "enabled": false, "value": { "maxNumber": 0 } } }, "id":

"b3c3d712-2c40-446f-ae9c-d99b742658ab", "links": { "self":

"/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/user-templates/b3c3d712-2c40-446f-
ae9c-d99b742658ab" },
```

```
"type": "userTemplate" } }
```

GET PowerShell Sample

```
########################################
#GET Specific User Settings Template


###
#Get Specific User Settings Templates
Write-Output "Get Specific User Settings Template"
Write-Output "-----"
$userTemplates = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-templates"
-Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($userTemplates in $userTemplates.id)
{
    Write-Output ("User Template found:  $($userTemplates.id):
$($userTemplates.attributes.name)")
}
$userTemplateID = $userTemplates.data[3].id


###
#Get Specific User Template
Write-Output "Get User Template for: "  $userTemplateID " with name: "
$userTemplate.data.attributes.name
Write-Output "-----"
$userTemplate = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates/$userTemplateID"
-Method 'GET' -Headers $authHeader
Write-Output $userTemplate | ConvertTo-Json -Depth 10
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/user-
templates/{userTemplateid}
```

PATCH Body Sample

```
### Get User Settings Template ### Need to obtain templates first
# @name userTemplates
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@userTemplateid = {{userTemplates.response.body.$.data[3].id}}
#Update the array to obtain the desired user template


### PATCH User Template by Template ID
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates/{{userTemplateid}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
    "data": {
        "type": "userTemplate",
        "attributes": {
            "enabled": false,
            "homeFolder": {
                "enabled": true,
                "value": {
                    "path": ""
                }
            }
        }
    }
}
```

PATCH Response Body Sample

```
{ "data": { "attributes": { "as2": { "inbound": { "enabled": true }, "outbound": {
"enabled": true } }, "changePassword": { "enabled": "inherit", "value": {
"changeAdminProvidedPasswordUponFirstUse": "inherit", "passwordExpiration": {
"enabled": true, "value": { "maxAgeDays": 90, "emailUpon": true, "remindPrior": {
"enabled": false, "value": { "daysBefore": 5, "emailUser": true } } } } } },
```

```
"connectionTimeout": { "enabled": true, "value": { "maxSec": 600 } },
"connectionsFromSameIpLimit": { "enabled": false, "value": { "maxNumber": 0 } },
"downloadSizeLimit": { "enabled": false, "value": { "maxKBytes": 0 } },
"downloadsPerSessionLimit": { "enabled": false, "value": { "maxNumber": 0 } },
"enabled": false, "ftp": { "enabled": true, "value": { "enableFxp": "inherit",
"enableNoop": "inherit", "enableComb": "yes", "enableXcrc": "yes", "enableZlib": true,
"banner": { "message": "Login OK. Proceed.", "usage": "replaceDefault" } } }, "ftps": {
"enabled": true }, "hasHomeFolderAsRoot": true, "homeFolder": { "enabled": true,
"value": {
...
"type": "userTemplate" } }
```


PATCH PowerShell Sample

```
#########################################################
##PATCH (Update) specific User Settings Template
###
#Get Specific User Settings Templates
Write-Output "Get Specific User Settings Template"
Write-Output "-----"
$userTemplates = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-templates" -
Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($userTemplates in $userTemplates.id)
{
    Write-Output ("User Template found:  $($userTemplates.id):
$($userTemplates.attributes.name)")
}
$userTemplateID = $userTemplates.data[3].id


###
#Get Specific User Template
Write-Output "Get User Template for: "  $userTemplateID " with name: "
$userTemplate.data.attributes.name
Write-Output "-----"
$userTemplate = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates/$userTemplateID"
-Method 'GET' -Headers $authHeader
Write-Output $userTemplate | ConvertTo-Json -Depth 10
```

```
###
##Patch Specific User Settings Template
Write-Output "User Settings Template Patch (update)"
Write-Output "-----"
$update =
'{
    "data":{
        "type": "userTemplate",
          "attributes": {
            "enabled": false,
            "homeFolder": {
                "enabled": true,
                "value": {
                    "path": ""
                }
            }
        }
    }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates/$userTemplateID"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/
{siteId}/user-templates/{userTemplateid}
```

DELETE Body Sample

```
###
#Delete Specific User Settings Template
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates/{{userTemplateid}}
HTTP/1.1
```

```
Authorization: EFTAdminAuthToken {{AuthToken}}
#
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Thu, 21 Jul 2022 13:38:16 GMT Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
############################################################
#Delete User Settings Template


#Get Specific User Settings Templates
Write-Output "Get Specific User Settings Template"
Write-Output "-----"
$userTemplates = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-templates"
-Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($userTemplates in $userTemplates.id)
{
    Write-Output ("User Template found:  $($userTemplates.id):
$($userTemplates.attributes.name)")
}
$userTemplateID = $userTemplates.data[3].id


###
#Get Specific User Template
Write-Output "Get User Template for: "  $userTemplateID " with name: "
$userTemplate.data.attributes.name
Write-Output "-----"
$userTemplate = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates/$userTemplateID"
-Method 'GET' -Headers $authHeader
```

```
Write-Output $userTemplate | ConvertTo-Json -Depth 10


#Delete Request

Write-Output "Deleting User Settings Template: "  $userTemplateID

Write-Output "-----"

$commandList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates/$userTemplateID"

-Method 'DELETE' -Headers $authHeader

Write-Output $commandList | ConvertTo-Json -Depth 10
```

Endpoint: /sites/{siteId}/user-groups

Note: Available as of EFT 8.1.0

Provides the ability to return a .list of user groups for a specific EFT site or create a new permission group.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups
```

GET Body Sample

```
### GET the User groups Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/userGroups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": [ { "attributes": { "name": "All Users" }, "id": "A0DB9377-92A3-4A38-8C0F-09F268D78FF1", "type": "userGroup" },
{ "attributes": { "name": "Administrators" }, "id": "07CACEB2-6698-4EF7-BAEB-F437FEC972A2", "type": "userGroup" },
{ "attributes": { "name": "Guests" }, "id": "B8448B77-01D8-47D5-8EE7-9F407C95E39F", "type": "userGroup" } ],
"links": { "self": "admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/userGroups" } }
```

GET PowerShell Sample

```
###GET User Groups###
Write-Output "GET User Groups"
Write-Output "-----------------"
#$siteID = "Enter site ID"
$Uglist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/userGroups" -Method 'GET' -Headers $authHeader
Write-Output $Uglist | ConvertTo-Json -Depth 25
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups
```

POST Body Sample

```
### Create User Permission Group ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
    "data": {
        "type": "userGroup",
        "attributes": {
            "name": "QA_API_User_Group_TEST"
        }
    }
}
```

POST Response Body Sample

```
{ "data": { "type": "userGroup", "id": "1ba8c63f-6e37-4783-b556-be5bf831dc6c",
"attributes": {
"name": "QA_API_User_Group_TEST" }, "relationships": { "users": { "data": [] } },
"links": {
"self": "/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/user-groups/1ba8c63f-6e37-
4783-b556-be5bf831dc6c" } } }
```

POST PowerShell Sample

```
#POST New Permission Group
Write-Output "POST User Permissions Group (New Permission Group)"
Write-Output "-----"
$update =
'{
  "data": {
        "type": "userGroup",
```

```
        "attributes": {
            "name": "QA_API_User_Group_TEST"
        }
    }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups"
-Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/user-groups/{groupid}

Note: Available as of EFT 8.1.0

Provides the ability to return a user group's details, update a permission group name or delete a user group.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups/{groupid}
```

GET Body Sample

```
### Get List of all User's Permissions Groups for the Site####
# @name UGlist
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@groupid = {{UGlist.response.body.$.data[3].id}}

### GET Details for specific User Permission Group####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups/{{groupid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": {
"type": "userGroup",
"id": "7386d09b-ac9d-42c8-a7dd-8ffb840d58e3",
"attributes": { "name": "QA_API_User_Group_TEST" },
"relationships": { "users": { "data": [] } },
"links": { "self":
```

```
"/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/user-groups/7386d09b-ac9d-42c8-
a7dd-8ffb840d58e3" } } }
```

GET PowerShell Sample

```
##########
#Get User Permission Groups
$userGroups = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups"
-Method 'GET' -Headers $authHeader
foreach ($userGroups in $userGroups.id)
{
    Write-Output ("User Permission Group found:  $($userGroups.id):
$($userGroups.attributes.name)")
}
$userGroupID = $userGroups.data[3].id



#Get Specific User Permission Group
Write-Output "Get Specific User Permission Group"
Write-Output "-----"
$userGroup = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups/$userGroupID"
-Method 'GET' -Headers $authHeader
Write-Output $userGroup | ConvertTo-Json -Depth 10
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/user-
groups/{groupid}
```

PATCH Body Sample

```
### GET Details for specific User Permission Group####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups/{{groupid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###

#### Update Name for Specific User Permissions Group
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}//user-groups/{{groupid}} HTTP/1.1
```

```
Authorization: EFTAdminAuthToken {{AuthToken}}


{
   "data": {
    "type": "userGroup",
    "attributes": {
      "name": "QA_API_User_Group_TEST2"
    }
  }
}
```

PATCH Response Body Sample

```
{ "data": {
"type": "userGroup",
"id": "7386d09b-ac9d-42c8-a7dd-8ffb840d58e3",
"attributes": { "name": "QA_API_User_Group_TEST2" },
"relationships": { "users": { "data": [] } }, "links": { "self":
"/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/user-groups/7386d09b-ac9d-42c8-
a7dd-8ffb840d58e3" } } }
```

PATCH PowerShell Sample

```
#Get Specific User Permission Group
Write-Output "Get Specific User Permission Group"
Write-Output "-----"
$userGroup = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups/$userGroupID"
-Method 'GET' -Headers $authHeader
Write-Output $userGroup | ConvertTo-Json -Depth 10


###
##Patch Specific User Permissions Group
Write-Output "User Permission Group Patch (update)"
Write-Output "-----"
$update =
'{
   "data": {
```

```
    "type": "userGroup",
    "attributes": {
      "name": "QA_API_User_Group_TEST2"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups/{groupid}

DELETE Body Sample

```
### Delete Specific User Permission Group ###
Delete https://{{host}}/admin/v2/sites/{{Siteid}}//user-groups/{{groupid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Fri, 22 Jul 2022 22:40:06 GMT Content-Length: 0 Cache-
Control: no-cache,
no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection:
1;
mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
#Get Specific User Permission Group
Write-Output "Get Specific User Permission Group"
Write-Output "-----"
```

```
$userGroup = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups/$userGroupID"
-Method 'GET' -Headers $authHeader
Write-Output $userGroup | ConvertTo-Json -Depth 10


###
#DELETE Specific User Permission Group
Write-Output "Delete Specific User Permission Group"
Write-Output "-----"
$commandList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID"
-Method 'DELETE' -Headers $authHeader
Write-Output $commandList | ConvertTo-Json -Depth 10
```

Endpoint: /sites/{siteId}/user-groups/{groupid}/relationships/users

Note: Available as of EFT 8.1.0

Provides the ability to return a user group's details, update a permission group name or delete a user group.

- POST
- DELETE

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups/{groupid}/relationships/users
```

POST Body Sample

```
###Get Users
# @name user
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@userid = {{user.response.body.$.data[3].id}}
#Store a user into a variable in order to add to a group later

###
### Get List of all User's Permissions Groups for the Site####
# @name UGlist
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@groupid = {{UGlist.response.body.$.data[3].id}}
#Store a user group in order to add a user to this group later

### Add User(s) to specific Permission Group ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups/
{{groupid}}/relationships/users HTTP/1.1
```

```
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": [
    {
      "type": "user",
      "id": "{{userid}}"
    }
   ]
}
```

POST Response Body Sample

```
{ "data": [ { "type": "user", "id": "b90be871-86ff-4060-b3cc-007903dff7f7",
"meta": { "name": "Ivan" } } ] }
```

POST PowerShell Sample

```
##
#Get User Permission Groups
$userGroups = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups" -Method
'GET' -Headers $authHeader
foreach ($userGroups in $userGroups.id)
{
Write-Output ("User Permission Group found:  $($userGroups.id):
$($userGroups.attributes.name)")
}
$userGroupID = $userGroups.data[3].id


###
#POST Selected User in Selected User Permission Group
Write-Output "POST (Add) User to Selected User Permissions Group"
Write-Output "-----"
$update =
'{
  "data": [
    {
```

```
      "type": "user",
      "id": "b90be871-86ff-4060-b3cc-007903dff7f7"
    }
   ]
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID/relationships/users"
-Method 'POST' -Headers $authHeader -Body $update
```

Method & URL

`DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups/{groupid}/relationships/users`

DELETE Body Sample

```
###Get Users
# @name user
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@userid = {{user.response.body.$.data[3].id}}
#Store a user into a variable in order to add to a group later

###
### Get List of all User's Permissions Groups for the Site####
# @name UGlist
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@groupid = {{UGlist.response.body.$.data[3].id}}
#Store a user group in order to add a user to this group later

### Delete User(s) from specific Permission Group ###
```

```
Delete https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups/{{groupid}}/
relationships/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": [
    {
      "type": "user",
      "id": "{{userid}}"
    }
  ]
}
```

DELETE Response Body Sample

```
HTTP/1.1 200 OK Date: Sat, 23 Jul 2022 01:47:11 GMT Content-Type:
application/vnd.api+json
Content-Length: 11 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer { "data": [] }
```

DELETE PowerShell Sample

```
##
#Get User Permission Groups
$userGroups = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups" -Method
'GET' -Headers $authHeader
foreach ($userGroups in $userGroups.id)
{
Write-Output ("User Permission Group found:  $($userGroups.id):
$($userGroups.attributes.name)")
}
$userGroupID = $userGroups.data[3].id


#Delete User from User Permission Group
Write-Output "Deleting User from User Permission Group: "
```

```
Write-Output "-----"
$update =
'{
  "data": [
    {
      "type": "user",
      "id": "b90be871-86ff-4060-b3cc-007903dff7f7"
    }
   ]
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$commandList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID/relationships/users"
-Method 'DELETE' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/ram/agents

Note: Available as of EFT 8.1.0

Returns a list of remote agents from a specified site.

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/ram/agents
```

GET Body Sample

```
### GET Remote Agents

GET  https://{{host}}/admin/v2/sites/{{Siteid}}/ram/agents HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

##
```

GET Response Body Sample


```
{ "data": [ { "id": "4dfd3f28-6ba9-4e19-ae7b-4d3b0b4314f6", "type": "remote-agent",
"attributes": {

"name": "ag_IV-2019A", "clid": "00000000-0000-0000-0000-000000000000", "state":
"PendingJoin",

"pausing": false, "resuming": false, "netBios": "IV-2019A", "domain": "", "winOEM": "x64
(AMD or Intel)",

"ips": [ "fe80::904:aa5a:7256:ca57 (Ethernet)", "10.91.160.123 (Ethernet)", "ff01::1
(Ethernet)",

"ff02::1 (Ethernet)", "ff02::c (Ethernet)", "ff02::fb (Ethernet)", "ff02::1:3
(Ethernet)",

"ff02::1:ff56:ca57 (Ethernet)", "224.0.0.1 (Ethernet)", "224.0.0.251 (Ethernet)",
"224.0.0.252 (Ethernet)",

"239.255.255.250 (Ethernet)", "::1 (Loopback Pseudo-Interface 1)", "127.0.0.1 (Loopback
Pseudo-Interface 1)",

"ff02::c (Loopback Pseudo-Interface 1)", "239.255.255.250 (Loopback Pseudo-Interface 1)"
],

"macAddresses": [ "0-15-5d-64-e-2c" ], "lastUpdate": 0, "version": "8.1.0.6",

"lastKnownIP": "10.91.160.123", "nextUpdate": 0, "approvedTime": 0,

"secret": "7102da9c0219696b82679072b9c2f", "peakVersion": "8.1.0.6" }, "links": {
"self":
```

```
"/admin/v2/sites/4ebb829f-f84c-4355-8d55-d43a2852ca12/ram/agents/4dfd3f28-6ba9-4e19-
ae7b-4d3b0b4314f6" } },

{ "id": "6ad61dcb-fabe-4627-aebe-065cfe4eadd0", "type": "remote-agent", "attributes": {
"name": "ag_IV-2019C",

"clid": "00000000-0000-0000-0000-000000000000", "state": "PendingJoin", "pausing":
false, "resuming": false,

"netBios": "IV-2019C", "domain": "", "winOEM": "x64 (AMD or Intel)", "ips": [


"fe80::2d7d:3dd6:4ff0:9bba (Ethernet)", "10.91.160.130 (Ethernet)", "ff01::1
(Ethernet)",

"ff02::1 (Ethernet)", "ff02::c (Ethernet)", "ff02::fb (Ethernet)", "ff02::1:3
(Ethernet)",

"ff02::1:fff0:9bba (Ethernet)", "224.0.0.1 (Ethernet)", "224.0.0.251 (Ethernet)",
"224.0.0.252 (Ethernet)",

"239.255.255.250 (Ethernet)", "::1 (Loopback Pseudo-Interface 1)", "127.0.0.1 (Loopback
Pseudo-Interface 1)",

"ff02::c (Loopback Pseudo-Interface 1)", "239.255.255.250 (Loopback Pseudo-Interface 1)"
],

"macAddresses": [ "0-15-5d-64-e-2e" ], "lastUpdate": 0, "version": "8.1.0.6",
"lastKnownIP": "10.91.160.130",

"nextUpdate": 0, "approvedTime": 0, "secret":
"0a8e8c89ed87352f0a979c73cb9e686ff3fe700a614546d28cbd96864e0de9fd",

"peakVersion": "8.1.0.6" }, "links": { "self": "/admin/v2/sites/4ebb829f-f84c-4355-8d55-
d43a2852ca12/ram/agents/

6ad61dcb-fabe-4627-aebe-065cfe4eadd0" } } ], "links": { "self": "/admin/v2/sites/

4ebb829f-f84c-4355-8d55-d43a2852ca12/ram/agents" } }
```


GET PowerShell Sample

```
# Get sites

$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites" -Method 'GET' -Headers
$authHeader

$siteID = $siteList.data[0].id


###GET Remote Agents

Write-Output "Remote Agents"

Write-Output "----"

$ramAgentList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ram/agents"

-Method 'GET' -Headers $authHeader

Write-Output $ramAgentList | ConvertTo-Json

foreach ($ramAgentList in $ramAgentList.data)

{
```

```
    Write-Output ("Remote Agent  $($ramAgentList.id): $($ramAgentList.attributes.name)")
}
```

Endpoint: /sites/{siteId}/ram/agents/{remoteAgentID}

Note: Available as of EFT 8.1.0

Returns a remote agent's settings from a specified site.

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ram/agents/{remoteAgentID}
```

GET Body Sample

```
### GET Remote Agents
# @name RAMList
GET  https://{{host}}/admin/v2/sites/{{Siteid}}/ram/agents HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
##
###
@remoteAgentID = {{RAMList.response.body.$.data[0].id}}


##
#Get Specific RAM Agent ID
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ram/agents/{{remoteAgentID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": { "id": "4dfd3f28-6ba9-4e19-ae7b-4d3b0b4314f6", "type": "remote-agent",
"attributes": {
"name": "ag_IV-2019A", "clid": "00000000-0000-0000-0000-000000000000", "state":
"PendingJoin",
"pausing": false, "resuming": false, "netBios": "IV-2019A", "domain": "", "winOEM": "x64
(AMD or Intel)",
"ips": [ "fe80::904:aa5a:7256:ca57 (Ethernet)", "10.91.160.123 (Ethernet)", "ff01::1
(Ethernet)", "ff02::1 (Ethernet)",
```

```
"ff02::c (Ethernet)", "ff02::fb (Ethernet)", "ff02::1:3 (Ethernet)", "ff02::1:ff56:ca57
(Ethernet)",

"224.0.0.1 (Ethernet)", "224.0.0.251 (Ethernet)", "224.0.0.252 (Ethernet)",
"239.255.255.250 (Ethernet)",

"::1 (Loopback Pseudo-Interface 1)", "127.0.0.1 (Loopback Pseudo-Interface 1)", "ff02::c
(Loopback Pseudo-Interface 1)",

"239.255.255.250 (Loopback Pseudo-Interface 1)" ], "macAddresses": [ "0-15-5d-64-e-2c"
], "lastUpdate": 0,

"version": "8.1.0.6", "lastKnownIP": "10.91.160.123", "nextUpdate": 0, "approvedTime":
0,

"secret": "7102da9c0219696b82679072b9c2f6e6d46fc0da9aa58d3fc1aa2e94f7858cde",
"peakVersion": "8.1.0.6" },

"links": { "self": "/admin/v2/sites/4ebb829f-f84c-4355-8d55-d43a2852ca12/ram/agents/

4dfd3f28-6ba9-4e19-ae7b-4d3b0b4314f6" } } }
```


GET PowerShell Sample

```
###GET Remote Agents

Write-Output "Remote Agents"

Write-Output "----"

$ramAgentList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ram/agents"

-Method 'GET' -Headers $authHeader

$ramAgentID = $ramAgentList.data[0].id


###GET Remote Agent Settings

Write-Output "GET Specific Remote Agent Settings: " $ramAgentID

Write-Output "----"

$ramAgent = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ram/agents/$ramAgentID"

-Method 'GET' -Headers $authHeader

Write-Output $ramAgent | ConvertTo-Json
```

Endpoint: /sites/{siteId}/ram/agents/templates

Note: Available as of EFT 8.1.0

Returns a remote agent template list from a specified site or allows the creation of a template on a specific EFT site.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/ram/templates
```

GET Body Sample

```
########################
#RAM TEMPLATES
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{ "data": [ { "id": "04cd2f6f-dea6-4674-bcde-3c7fe5a800a1", "type": "remote-agents-
template",
"attributes": { "name": "RAM Template1", "updateInterval": "EveryFiveMinutes",
"eventRuleIds": [ null, "d352632d-5f3f-49bf-99af-849f7453dd0a" ], "autoEnroll": false,
"autoEnrollDate": 1659757989, "homeFolder": "/Usr/Agents/%AgentNetBIOSName%/",
"updateFailure":
"Stop_Disable_Unenroll", "enableIPAccess": false, "ipAccess": { "masks": [ { "ipMask":
"0.0.0.0",
"reason": "", "matchAction": "Deny", "timeStamp": 0, "autobanEntry": true } ],
"autoban": [],
"defaultAction": "Allow" } }, "links": { "self": "/admin/v2/sites/
4ebb829f-f84c-4355-8d55-d43a2852ca12/ram/templates/04cd2f6f-dea6-4674-bcde-3c7fe5a800a1"
} }, {
"id": "b672dec5-567e-4baa-bc3f-5be948802b42", "type": "remote-agents-template",
"attributes": {
"name": "RAM Template 2", "updateInterval": "EveryFiveMinutes", "eventRuleIds": [ null,
```

```
"d352632d-5f3f-49bf-99af-849f7453dd0a" ], "autoEnroll": false, "autoEnrollDate":
1659761201,

"homeFolder": "/Usr/Agents/%AgentNetBIOSName%/", "updateFailure": "Stop_Disable_
Unenroll",

"enableIPAccess": true, "ipAccess": { "masks": [ { "ipMask": "10.15.25.35", "reason":
"TEst BAN",

"matchAction": "Allow", "timeStamp": 1658551620, "autobanEntry": false }, { "ipMask":
"0.0.0.0",

"reason": "", "matchAction": "Deny", "timeStamp": 0, "autobanEntry": true } ],
"autoban": [],

"defaultAction": "Allow" } }, "links": { "self": "/admin/v2/sites/4ebb829f-f84c-4355-
8d55-d43a2852ca12/ram/templates/

b672dec5-567e-4baa-bc3f-5be948802b42" } } ], "links": { "self": "/admin/v2/sites/

4ebb829f-f84c-4355-8d55-d43a2852ca12/ram/templates" } }
```


GET PowerShell Sample

```
################

##GET Remote Agent Templates

Write-Output "Remote Agent Templates"

Write-Output "----"

$ramTemplateList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ram/templates"

-Method 'GET' -Headers $authHeader

Write-Output $ramTemplateList | ConvertTo-Json -Depth 10

foreach ($ramTemplateList in $ramTemplateList.data)

{

    Write-Output ("Remote Agent Template  $($ramTemplateList.id):
$($ramTemplateList.attributes.name)")

}
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/
{siteId}/ram/templates
```

POST Body Sample

```
### Add New RAM Template ###

POST https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates HTTP/1.1
```

```
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "attributes": {
      "name": "NewRAMTemplateName",
      "updateInterval": "EveryFiveMinutes",
      "eventRuleIds": [
        "d352632d-5f3f-49bf-99af-849f7453dd0a"
      ],
      "autoEnroll": true,
      "autoEnrollDate": 0,
      "homeFolder": "/Usr/Agents/%AgentNetBIOSName%/",
      "updateFailure": "Stop_Disable_Unenroll",
      "enableIPAccess": true,
      "ipAccess": {
        "masks": [
          {
            "ipMask": "0.0.0.0",
            "reason": "",
            "matchAction": "Deny",
            "timeStamp": 0,
            "autobanEntry": true
          }
        ],
        "defaultAction": "Allow"
      }
    }
  }
}
```

POST Response Body Sample

```
{ "data": { "id": "b3ed1f50-ce61-479f-ba48-094cee3c13fd", "type": "remote-agents-
template", "attributes": {
"name": "NewRAMTemplateName", "updateInterval": "EveryFiveMinutes", "eventRuleIds": [
null,
```

```
"d352632d-5f3f-49bf-99af-849f7453dd0a" ], "autoEnroll": true, "autoEnrollDate": 0,
"homeFolder":

"/Usr/Agents/%AgentNetBIOSName%/", "updateFailure": "Stop_Disable_Unenroll",
"enableIPAccess": true,

"ipAccess": { "masks": [ { "ipMask": "0.0.0.0", "reason": "", "matchAction": "Deny",
"timeStamp": 0,

"autobanEntry": false } ], "autoban": [], "defaultAction": "Allow" } }, "links": {
"self":

"/admin/v2/sites/4ebb829f-f84c-4355-8d55-d43a2852ca12/ram/templates/b3ed1f50-ce61-479f-
ba48-094cee3c13fd" } } }
```


POST PowerShell Sample

```
#######

###

#POST New RAM Template

Write-Output "POST RAM Template"

Write-Output "-----"

$update =

'{

  "data": {

    "attributes": {

      "name": "NewRAMTemplateName",

      "updateInterval": "EveryFiveMinutes",

      "eventRuleIds": [

        "d352632d-5f3f-49bf-99af-849f7453dd0a"

      ],

      "autoEnroll": true,

      "autoEnrollDate": 0,

      "homeFolder": "/Usr/Agents/%AgentNetBIOSName%/",

      "updateFailure": "Stop_Disable_Unenroll",

      "enableIPAccess": true,

      "ipAccess": {

        "masks": [

          {

            "ipMask": "0.0.0.0",

            "reason": "",

            "matchAction": "Deny",

            "timeStamp": 0,
```

```
            "autobanEntry": true
          }
        ],
        "defaultAction": "Allow"
      }
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ram/templates"
-Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/ram/agents/templates/{remoteAgentsTemplateID}

Note: Available as of EFT 8.1.0

Returns a remote agent settings template from a specified site, update/patch a remote agent settings template, or allows the deletion of a remote agent settings template on a specific EFT site.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/ram/templates/{remoteAgentsTemplateID}
```

GET Body Sample

```
############################
#GET RAM Template by ID
#RAM TEMPLATES
# @name RAMTemplates
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@ramTemplateID = {{RAMTemplates.response.body.$.data[0].id}}

###
#GET Template by Template ID
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates/{{ramTemplateID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{ "data": { "id": "04cd2f6f-dea6-4674-bcde-3c7fe5a800a1", "type": "remote-agents-
template",

"attributes": { "name": "RAM Template1", "updateInterval": "EveryFiveMinutes",

"eventRuleIds": [], "autoEnroll": false, "autoEnrollDate": 1659757989,

"homeFolder": "/Usr/Agents/%AgentNetBIOSName%/", "updateFailure": "Stop_Disable_
Unenroll",

"enableIPAccess": false, "ipAccess": { "masks": [ { "ipMask": "0.0.0.0", "reason": "",

"matchAction": "Deny", "timeStamp": 0, "autobanEntry": false } ], "autoban": [],
"defaultAction":

"Allow" } }, "links": { "self": "/admin/v2/sites/4ebb829f-f84c-4355-8d55-
d43a2852ca12/ram/

templates/04cd2f6f-dea6-4674-bcde-3c7fe5a800a1" } } }
```


GET PowerShell Sample

```
################

##GET Remote Agent Templates

$ramTemplateList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ram/templates" -
Method 'GET'

-Headers $authHeader

$ramTemplateID = $ramTemplateList.data[0].id


####

#GET Remote Agent Template by ID

Write-Output "Remote Agent Template by ID: " $ramTemplateID

Write-Output "----"

$ramTemplate = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates/$ramTemplateID" -Method 'GET'

-Headers $authHeader

Write-Output $ramTemplate | ConvertTo-Json -Depth 10
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/ram/templates/{remoteAgentsTemplateID}
```

PATCH Body Sample

```
####

#PATCH Template by Template ID

PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates/{{ramTemplateID}}
HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "attributes": {
        "ipAccess": {
        "masks": [
          {
            "ipMask": "0.0.0.0",
            "reason": "",
            "matchAction": "Deny",
            "timeStamp": 0,
            "autobanEntry": false
          }
        ],
        "defaultAction": "Allow"
      }
    }
  }
}
```

PATCH Response Body Sample

```
{ "data": { "id": "04cd2f6f-dea6-4674-bcde-3c7fe5a800a1", "type": "remote-agents-
template",

"attributes": { "name": "RAM Template1", "updateInterval": "EveryFiveMinutes",

"eventRuleIds": [], "autoEnroll": false, "autoEnrollDate": 1659757989, "homeFolder":

"/Usr/Agents/%AgentNetBIOSName%/", "updateFailure": "Stop_Disable_Unenroll",

"enableIPAccess": false, "ipAccess": { "masks": [ { "ipMask": "0.0.0.0", "reason": "",

"matchAction": "Deny", "timeStamp": 0, "autobanEntry": false } ], "autoban": [],

"defaultAction": "Allow" } }, "links": { "self": "/admin/v2/sites/

4ebb829f-f84c-4355-8d55-d43a2852ca12/ram/templates/04cd2f6f-dea6-4674-bcde-3c7fe5a800a1"
} } }
```

PATCH PowerShell Sample

```
##########
##GET Remote Agent Template ID
$ramTemplateList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ram/templates"
-Method 'GET' -Headers $authHeader
$ramTemplateID = $ramTemplateList.data[0].id

###
##Patch Remote Agent Template by ID
Write-Output "Remote Agent Template Patch (update)"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes": {
        "ipAccess": {
        "masks": [
          {
            "ipMask": "1.1.1.1",
            "reason": "",
            "matchAction": "Deny",
            "timeStamp": 0,
            "autobanEntry": false
          }
        ],
        "defaultAction": "Allow"
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates/$ramTemplateID"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/
{siteId}/ram/templates/{remoteAgentsTemplateID}
```

DELETE Body Sample

```
####

#DELETE Remote Agent Template

#Template must not have existing associated Remote Agents

DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates/{{ramTemplateID}}
HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Sun, 24 Jul 2022 02:05:46 GMT Content-Length: 0

Cache-Control: no-cache, no-store, must-revalidate Expires: -1

X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;

Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
#####################################

##########

##GET Remote Agent Template ID

$ramTemplateList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ram/templates"

-Method 'GET' -Headers $authHeader

$ramTemplateID = $ramTemplateList.data[1].id


####

#DELETE Remote Agent Template by ID

$ramTemplateList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates/$ramTemplateID"

-Method 'DELETE' -Headers $authHeader
```

Endpoint:/sites/{siteId}/awe-tasks

Note: Available as of EFT 8.1.0

(GET) Returns advanced workflow task list from specified site and (POST) creates advanced workflow task for specified site

- GET
- POST

Method & URL

```
GET https://{{host}}/admin/v2/sites/{{SiteId}}/awe-tasks
```

GET Body Sample

```
### GET AWE TASKS ###

GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample


```
{"data":[{"id":"0f340ef3-3628-5844-bb6b-c659252b6b44","type":"aweTask",

"attributes":{"name":"Sample - Date Format Functions","created":"2022-08-01",

"description":""},"relationships":{"aweFolder":{"data":{"id":"00000000-0000-0000-0000-
000000000000",

"name":"<root>"}}},"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-
477c08f0abca/awe-tasks/

0f340ef3-3628-5844-bb6b-c659252b6b44"}},{"id":"92ac1ba6-5fcc-5b85-b5da-e1b3c4d4a300",

"type":"aweTask","attributes":{"name":"Sample - Environment Variables","created":"2022-
08-01",

"description":""},"relationships":{"aweFolder":{"data":{"id":"00000000-0000-0000-0000-
000000000000",

"name":"<root>"}}},"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-
477c08f0abca/

awe-tasks/92ac1ba6-5fcc-5b85-b5da-e1b3c4d4a300"}},{"id":"432c99b4-fcf3-5472-981d-
416946a9b95a",

"type":"aweTask","attributes":{"name":"Sample - Excel Actions","created":"2022-08-01",

"description":""},"relationships":{"aweFolder":{"data":{"id":"00000000-0000-0000-0000-
000000000000",
```

```
"name":"<root>"}}},"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-
477c08f0abca/

awe-tasks/432c99b4-fcf3-5472-981d-416946a9b95a"}},{"id":"df5f43bb-1f34-57be-9e59-
75bd272ba408",

"type":"aweTask","attributes":{"name":"Sample -
```


GET PowerShell Sample

```
# get awe-tasks

Write-Output "AWE-TASKS"

Write-Output "-----"

$aweList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks"

-Method 'GET' -Headers $authHeader

Write-Output $aweList | ConvertTo-Json

foreach ($awetask in $aweList.data)

{

    Write-Output ("Task ID $($aweTask.id): Name -> $($aweTask.attributes.name)")

}
```

Method & URL

```
POST https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks
```

POST Body Sample

```
POST https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}


{

  "data": {

    "type": "aweTask",

    "attributes": {

    "code":"PEFNVEFTSz4NCjxBTVRBU0tIRUFEPg0KICAgIDxUQVNLSU5GTyBUQVNLVkVSU0lPTj0iMTAuNy4x
MDAuMSI...Vt",

      "name": "MyNewAWEScript",

      "created": "2022-03-31",

      "description": "Hello, world!",

      "useTimeout": true,

      "timeout": 10,
```

```
      "logLevel": "Verbose",
      "retainSuccessfulLogs": false,
      "retainFailedLogs": true
    }
  }
}
```

POST Response Body Sample

```
{"data":{"id":"8405b064-aa9a-46b8-b0b5-4c60eb3d3e09","type":"aweTask","attributes":
{"name":"MyNewAWEScript",
"created":"2022-08-01","description":"Hello,
world!","useTimeout":true,"timeout":10,"logLevel":"Verbose",
"logDirectory":"","retainSuccessfulLogs":false,"retainFailedLogs":true,
"code":"PEFNVEFTSz4NCjxBTVRBU0tIRUFEPg0KICAgIDxUQVNLSU5GTyBUQVNLVkVS...s+DQo="},"relatio
nships":
{"aweFolder":{"data":{"id":"00000000-0000-0000-0000-000000000000","name":"<root>"}}},
"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks/
8405b064-aa9a-46b8-b0b5-4c60eb3d3e09"}},
"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks"}}
```

POST PowerShell Sample

```
##POST SITE AWE TASKS
Write-Output "Site AWE TASK POST"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "aweTask",
    "attributes": {
    "code":"PEFNVEFTSz4NCjxBTVRBU0tIRUFEPg0KICAgIDxUQVNLSU5GTyBUQVNLV...+DQo=",
      "name": "MyNewAWEScript",
      "created": "2022-03-31",
      "description": "Hello, world!",
      "useTimeout": true,
      "timeout": 10,
```

```
      "logLevel": "Verbose",
      "retainSuccessfulLogs": false,
      "retainFailedLogs": true
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$postAWETASKReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks"
-Method 'POST' -Headers $authHeader -Body $update
Write-Output $postAWETASKReturn | ConvertTo-Json
```

Endpoint:/sites/{siteId}/awe-tasks/{aweTaskID}

Note: Available as of EFT 8.1.0

(GET) Returns advanced workflow task from specified site, (PATCH) Updates advanced workflow task settings, and (DELETE) Delete advanced workflow task

- GET
- PATCH
- DELETE

Method & URL

```
GET https://{{host}}/admin/v2/sites/{{SiteId}}/awe-tasks/
{aweTaskID}
```

GET Body Sample

```
### GET A SPECIFIC AWE TASK

@aweID = {{aweList.response.body.$.data[0].id}}

GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks/{{aweID}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample


```
{"data":{"id":"0f340ef3-3628-5844-bb6b-c659252b6b44","type":"aweTask",

"attributes":{"name":"Sample - Date Format Functions","created":"2022-08-
01","description":"",

"useTimeout":true,"timeout":120,"logLevel":"None","logDirectory":

"C:\\ProgramData\\Globalscape\\EFT Server\\AWE\\Temp\\","retainSuccessfulLogs":true,

"retainFailedLogs":true,"code":"PEFNVEFTSz4NCjxBTVRBU0tIRUFEPg0KICAgIDxUQVNLSU5GTyBUQVNL
VkVSU0lPTj0

jxBTUZVTkNUSU9OIE5BTUU9Ik9uU3RlcEVycm9yIiBBQ0NFU1M9InByaXZhdGUiPg0KPEFNUEFSQU1FVEVSIE5BT
UU9IkZ1bmN

0aW9uTmFtZSIgREVTQ1JJUFRJT049IlRoZSBmdW5jdGlvbiB3aXRoIHRoZSBlcnJvciIgU1VCVFlQRT0idGV4dCI
gLz4NCjxBTV

BBUkFNRVRFUiBOQU1FPSJTdGVwTnVtYmVyIiBERVNDUklQVElPTj0iVGhlIHN0ZXAgbnVtYmVyIG9mIHRoZSBlcn
JvciIgU
```

```
1VCVFlQRT0ibnVtYmVyIiAvPg0KPEFNUEFSQU1FVEVSIE5BTUU9IkVycm9yVGV4dCIgREVTQ1JJUFRJT049IlRoZSB0ZXh0I

...

s+DQo="},"relationships":{"aweFolder":{"data":{"id":"00000000-0000-0000-0000-000000000000","name":"<root>"}}},

"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks/0f340ef3-3628-5844-bb6b-c659252b6b44"}},

"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks"}}
```


GET PowerShell Sample

```
# get awe-tasks
Write-Output "AWE-TASKS"
Write-Output "-----"
$aweList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks"
-Method 'GET' -Headers $authHeader
Write-Output $aweList | ConvertTo-Json
foreach ($awetask in $aweList.data)
{
    Write-Output ("Task ID $($aweTask.id): Name -> $($aweTask.attributes.name)")
}

$aweID = $aweList.data[0].id
$awsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks/$aweID"
-Method 'GET' -Headers $authHeader
Write-Output $awsList | ConvertTo-Json
```

Method & URL

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks/{{aweID}}
```

PATCH Body Sample

```
### UPDATE A SPECIFIC AWE TASK (this is using the environment var code)
### for your site you may have to adjust the index number
@aweID = {{aweList.response.body.$.data[14].id}}
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks/{{aweID}} HTTP/1.1
```

```
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "aweTask",
    "attributes": {
      "logDirectory": "C\\temp\\"
    }
  }
}
###
```

PATCH Response Body Sample


```
{"data":{"id":"8405b064-aa9a-46b8-b0b5-4c60eb3d3e09","type":"aweTask","attributes":
{"name":"MyNewAWEScript",

"created":"2022-08-01","description":"Hello,
world!","useTimeout":true,"timeout":10,"logLevel":"Verbose",

"logDirectory":"C\\temp\\","retainSuccessfulLogs":false,"retainFailedLogs":true,"code":

"PEFNVEFTSz4NCjxBTVRBU0tIRUFEPg0KICAgIDxUQVNLSU5GTyBUQVNLVkVSU0lPTj0iMTAuNy4xMDAuMSIgLz4
NCjwvQU1UQVNLSE

...

NVQlRZUEU9InRleHQiIC8+DQoNCjwvQU1GVU5DVElPTj4NCg0KPC9BTVRBU0s+DQo="},"relationships":
{"aweFolder":{

"data":{"id":"00000000-0000-0000-0000-000000000000","name":"<root>"}}},"links":
{"self":"/admin/v2/sites

/b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks/8405b064-aa9a-46b8-b0b5-
4c60eb3d3e09"}},"links":{"self":"/

admin/v2/sites/b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks"}}
```


PATCH PowerShell Sample

```
##PATCH SITE AWE TASKS

Write-Output "Site specific AWE TASK PATCH"

Write-Output "-----"

$update =

'{
  "data": {
    "type": "aweTask",
```

```
    "attributes": {
      "description": "Well Hello",
      "useTimeout": true,
      "timeout": 10,
      "logLevel": "Verbose",
      "retainSuccessfulLogs": true,
      "retainFailedLogs": true
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchAWETASKReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-
tasks/$aweID"
-Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $patchAWETASKReturn | ConvertTo-Json
```

Method & URL

```
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks/
{{aweID}}
```

DELETE Body Sample

```
### DELETE A SPECIFIC AWE TASK
@aweID = {{aweList.response.body.$.data[0].id}}

DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks/{{aweID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content
Date: Mon, 01 Aug 2022 21:16:00 GMT
Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate
```

```
Expires: -1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
$aweID = $aweList.data[0].id
$awsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks/$aweID"
-Method 'DELETE' -Headers $authHeader
Write-Output $awsList | ConvertTo-Json
```

Endpoint:/sites/{siteId}/awe-tasks-folders

Note: Available as of EFT 8.1.0

(GET) Returns advanced workflow folder list from specified site and (POST) create advanced workflow folder for specified site

- GET
- POST

Method & URL

```
GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-task-folders
```

GET Body Sample

```
### GET ALL AWE TASK FOLDERS ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{"data":[{"id":"00000000-0000-0000-0000-000000000000","type":"aweFolder","attributes":{
"name":"<root>","tasks":[{"id":"92ac1ba6-5fcc-5b85-b5da-e1b3c4d4a300","name":
"Sample - Environment Variables","created":"2022-08-01","description":""},{"id":
"432c99b4-fcf3-5472-981d-416946a9b95a","name":"Sample - Excel Actions","created":"2022-
08-01",
"description":""},{"id":"df5f43bb-1f34-57be-9e59-75bd272ba408","name":"Sample -
Expectations",
"created":"2022-08-01","description":""},{"id":"cf774000-2d0a-5962-a060-111aa4d94d1c",
"name":"Sample - File Date Operations","created":"2022-08-01","description":""},{
"id":"40536ad8-327e-53d6-8566-0d7722156b42","name":"Sample - FTP
Actions","created":"2022-08-01",
"description":""},{"id":"a6a79232-f9e5-5a14-b944-d7922e275fd0","name":"Sample - If and
Else and EndIf",
"created":"2022-08-01","description":""},{"id":"27c02e7e-ef14-5c1f-b694-50e3ad672ae3",
"name":"Sample - Ping","created":"2022-08-01","description":""},{"id":
"dc274226-442e-5ee4-b968-35e5ebfbd521","name":"Sample - Query a CSV
File","created":"2022-08-01",
```

```
"description":""},{"id":"5cd49fc4-4f4d-5369-9901-d785aebf4f38","name":"Sample - Run
Embedded Script",

"created":"2022-08-01","description":""},{"id":"e61f958c-c541-5dc6-8f75-
4ee68a9601e1","name":

"Sample - Send E-mail","created":"2022-08-01","description":""},{"id":

"c72543b2-9374-5e9e-9fd6-85befa3dcf73","name":"Sample - Sites and Users through COM",

"created":"2022-08-01","description":""},{"id":"d9f234c1-cb38-5afe-9416-71c33a2987c8",

"name":"Sample - Terminal Emulation","created":"2022-08-01","description":""},{"id":

"c6b17e66-598b-5838-a3fd-b671e93bafb6","name":"Sample - _README FIRST_","created":"2022-
08-01",

"description":""},{"id":"8405b064-aa9a-46b8-b0b5-4c60eb3d3e09","name":"MyNewAWEScript",

"created":"2022-08-01","description":"Hello, world!"}]},"links":{"self":

"/admin/v2/sites/b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks-folders/

00000000-0000-0000-0000-000000000000"}},{"id":"793e3b44-cb54-47db-8116-
9bc45a50d158","type":"aweFolder",

"attributes":{"name":"AWE_Folder_Two","tasks":[]},"links":{"self":"/admin/v2/sites/

b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks-folders/793e3b44-cb54-47db-8116-
9bc45a50d158"}},{

"id":"859dc605-0600-42ab-a1fa-f23f5a19e8cd","type":"aweFolder","attributes":{

"name":"AWE _ Folder_One","tasks":[]},"links":{"self":"/admin/v2/sites/

b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks-folders/859dc605-0600-42ab-a1fa-
f23f5a19e8cd"}}],

"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks-
folders"}}
```


GET PowerShell Sample

```
####Added 2/01/2020

### Returns all site auto ban list###

Write-Output "AWE Task Folders"

Write-Output "----"

$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-folders"

-Method 'GET' -Headers $authHeader

Write-Output $siteList | ConvertTo-Json
```

Method & URL

```
POST https://{{host}}/admin/v2/sites/{{Siteid}}/awe-task-folders
```

POST Body Sample

```
### create a folder named AWE_Folder_Three
###


###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "type": "aweTaskFolder",
    "attributes": {
      "name": "AWE_Folder_Three"
    }
  }
}
###
```

POST Response Body Sample

```
{"data":{"id":"dc70ad42-47ad-4239-a81a-fe9d650820aa","type":"aweFolder","attributes":{
"name":"AWE_Folder_Three","tasks":[]},"links":{"self":"/admin/v2/sites/
b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks-folders/dc70ad42-47ad-4239-a81a-
fe9d650820aa"}},
"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks-
folders"}}
```

POST PowerShell Sample

```
####Added 2/01/2020
### Returns all site auto ban list###
Write-Output "AWE Task Folders"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-folders"
-Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

```
##POST SITE AWE TASKS FOLDERS
Write-Output "Site AWE TASK FOLDER POST"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "aweTaskFolder",
    "attributes": {
      "name": "AWE_Folder_FIVE-O"
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$postAWETASKReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-
folders"
-Method 'POST' -Headers $authHeader -Body $update
Write-Output $postAWETASKReturn | ConvertTo-Json
```

Endpoint:/sites/{sitetId}/awe-tasks-folders/{aweTaskFolderID}

Note: Available as of EFT 8.1.0

(GET) Returns advanced workflow folder from specified site, (PATCH) Updates advanced workflow folder settings, and (DELETE) Delete advanced workflow folder.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders/{{AWEId}}
```

GET Body Sample

```
### GET A SPECIFIC AWE TASK FOLDERS ###

@AWEId = 859dc605-0600-42ab-a1fa-f23f5a19e8cd

GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders/{{AWEId}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample


```
{"data":{"id":"859dc605-0600-42ab-a1fa-f23f5a19e8cd","type":"aweFolder","attributes":
{"name":

"AWE _ Folder_One","tasks":[]},"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-
477c08f0abca/

awe-tasks-folders/859dc605-0600-42ab-a1fa-f23f5a19e8cd"}},"links":
{"self":"/admin/v2/sites/

b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks-folders"}}
```


GET PowerShell Sample

```
####Added 2/01/2020

### Returns awe folder information###

Write-Output "AWE Task Folders"

Write-Output "----"

$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-folders" -Method
'GET'

-Headers $authHeader

Write-Output $siteList | ConvertTo-Json


$aweID = $siteList.data[1].id

Write-Output "----"

$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-folders/$aweID"
-Method 'GET'

-Headers $authHeader

Write-Output $siteList | ConvertTo-Json
```

Method & URL

```
PATCH  https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-
folders/{{AWEId}}
```

PATCH Body Sample

```
@AWEId = dc70ad42-47ad-4239-a81a-fe9d650820aa

### PATCH AWE TASK FOLDERS ###

PATCH  https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders/{{AWEId}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "id": "dc70ad42-47ad-4239-a81a-fe9d650820aa",
    "attributes": {
      "name": "NewFirstFolder"
    },
    "type": "aweTaskFolder"
  }
```

```
}
###
```

PATCH Response Body Sample

```
{"data":{"id":"dc70ad42-47ad-4239-a81a-fe9d650820aa","type":"aweFolder","attributes":
{"name":
"NewFirstFolder","tasks":[{"id":"432c99b4-fcf3-5472-981d-416946a9b95a","name":
"Sample - Excel Actions","created":"2022-08-01","description":"My Description"},{
"id":"40536ad8-327e-53d6-8566-0d7722156b42","name":"Sample - FTP Actions","created":
"2022-08-01","description":""}]},"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-
a3b1-477c08f0abca/
awe-tasks-folders/dc70ad42-47ad-4239-a81a-fe9d650820aa"}},"links":
{"self":"/admin/v2/sites/
b65892e9-399d-4447-a3b1-477c08f0abca/awe-tasks-folders"}}
```

PATCH PowerShell Sample

```
$folderID = $aweFolderList.data[1].id


##POST SITE AWE TASKS FOLDERS
Write-Output "Site AWE TASK FOLDER PATCH"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "aweTaskFolder",
    "attributes": {
      "name": "TEST FOLDER TWO"
    }
  }
}'


$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchAWETASKReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-
folders/$folderID"
-Method 'PATCH' -Headers $authHeader -Body $update
```

```
Write-Output $patchAWETASKReturn | ConvertTo-Json
```

Method & URL

`DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders/{{AWEId}}`

NOTE: The folder should be emptied before it is deleted else the EFT will return a HTTP 500 Server error.

DELETE Body Sample

```
### AWEId will be the id of a folder to be deleted.
@AWEId = e1d62bf1-8bdd-4e82-8efd-395467069306
### DELETE AWE TASK FOLDERS ###
DELETE  https://{{host}}/admin/v2/sites/{{Siteid}}/awe-task-folders/{{AWEId}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content
Date: Tue, 02 Aug 2022 17:47:50 GMT
Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate
Expires: -1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
$folderID = $aweFolderList.data[1].id
```

```
$deleteAWETASKReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-
folders/$folderID"

-Method 'DELETE' -Headers $authHeader

Write-Output $deleteAWETASKReturn | ConvertTo-Json
```

Endpoint: /sites/{siteId}/connection-profiles

Note: Available as of EFT 8.1.0

- GET - Returns connection profiles list from the specified site.
- POST - Creates a connection profile for a site.

Method & URL

```
GET https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles
```

GET Body Sample

```
### GET a list of current connection profiles####

GET https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Thu, 04 Aug 2022 14:17:24 GMT Location:

/admin/v2/sites/76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles

Content-Type: application/vnd.api+json Content-Length: 1383 Cache-Control:

no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection: 1;

mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;

Referrer-Policy: no-referrer { "data": [ { "id": "c9ea36ec-8a9e-440f-8c21-920eb3927732", "type":

"connectionProfile", "attributes": { "type": "Protocol", "name": "POST REQUEST Create connection Profile",

"description": "Connection Profile Details", "connectionSettings": { "protocol": "FTPSAuthTLS", "user":

"AFAR", "password": "UpKUJq1sD4Yfb1Hz8ZFiRw==", "autoLogin": true, "testPath": "\test", "host":

"192.168.1.210", "port": 21, "SSLCertificate": { "certPath": "", "keyPath": "", "passphrase":

"UpKUJq1sD4Yfb1Hz8ZFiRw==" }, "trustedPubKey": "", "proxy": { "use": false, "type": "FTP",
```

```
"hostName": "", "username": "", "password": "UpKUJq1sD4Yfb1Hz8ZFiRw==", "port": 21,
"subType": 0,

"separator": "@", "customCommands": [] }, "socks": { "use": false, "type": "None",
"hostName": "",

"port": 1080, "auth": false, "username": "", "password": "UpKUJq1sD4Yfb1Hz8ZFiRw==" },
"advanced":

{ "numberOfConnectionRetries": 0, "delayBetweenRetries": 30, "maxConcurrentThreads": 1,

"connectionTimeout": 30, "port": { "mode": "AUTO", "min": 0, "max": 65535 },
"validateFileIntegrity":

false, "ASCIIFileExts": [ "TXT", "INF", "HTML", "HTM" ], "homeIP": "0.0.0.0",
"clearCommandChannel":

false, "clearDataChannel": false, "transferEncoding": "AutoDetect", "timeStamp": {
"preserveLocal":

false, "preserveRemote": false } } } }, "links": { "self":

"/admin/v2/sites/76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles/c9ea36ec-8a9e-
440f-8c21-920eb3927732"

} } ], "links": { "self": "/admin/v2/sites/76882fc7-3f55-4040-ae5f-
2e645c12647b/connection-profiles"

}

}
```


GET PowerShell Sample

```
#####################################

###GET list of Connection Profiles###

Write-Output "GET list of Connection Profiles"

Write-Output "------------------------------"

#$siteID = "Enter site ID"

$CPlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/connection-Profiles" -Method
'GET'

-Headers $authHeader

Write-Output $CPlist | ConvertTo-Json -Depth 25

$profileId = $CPList.data[0].id
```

Method & URL

```
POST https://{{host}}/admin/v2/sites/{{Siteid}}/connection-
Profiles
```

POST Body Sample

```
### Create a Connection Profile ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "connectionProfile",
    "attributes": {
      "name": "POST REQUEST Create connection Profile",
      "description": "Connection Profile Details",
      "testPath": "\test",
      "connectionSettings": {
        "protocol": "FTPSAuthTLS",
        "host": "192.168.1.210",
        "port": 21,
        "user": "AFAR",
        "password": "",
        "autoLogin": true,
        "certSettings": {
          "certPath": "C:\\Users\\Administrator\\Desktop\\AFAR SSL\\SSL Cert User
AFAR.crt",
          "keyPath": "C:\\Users\\Administrator\\Desktop\\AFAR SSL\\SSL Cert User
AFAR.key",
          "passphrase": "xamYEctkRdBRCxu0F5XqoQ=="
        }
      }
    }
 }
```

POST Response Body Sample

```
HTTP/1.1 201 Created Date: Thu, 04 Aug 2022 15:51:07 GMT Location:
/admin/v2/sites/76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles/
92e9f684-5b87-47d3-816b-19644e639ae2 Content-Type: application/vnd.api+json
ETag: "24708EE" Content-Length: 1290 Cache-Control: no-cache, no-store, must-revalidate
Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
```

```
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;

Referrer-Policy: no-referrer { "data": { "id": "92e9f684-5b87-47d3-816b-19644e639ae2",

"type": "connectionProfile", "attributes": { "type": "Protocol",

"name": "POSTq REQUEST Create connection Profile", "description": "Connection Profile
Details",

"connectionSettings": { "protocol": "FTPSAuthTLS", "user": "AFAR", "password":
"UpKUJq1sD4Yfb1Hz8ZFiRw==",

"autoLogin": true, "testPath": "\test", "host": "192.168.1.210", "port": 21,
"SSLCertificate": {

"certPath": "", "keyPath": "", "passphrase": "UpKUJq1sD4Yfb1Hz8ZFiRw==" },
"trustedPubKey": "",

"proxy": { "use": false, "type": "FTP", "hostName": "", "username": "", "password":
"UpKUJq1sD4Yfb1Hz8ZFiRw==",

"port": 21, "subType": 0, "separator": "@", "customCommands": [] }, "socks": { "use":
false,

"type": "None", "hostName": "", "port": 1080, "auth": false, "username": "",

"password": "UpKUJq1sD4Yfb1Hz8ZFiRw==" }, "advanced": { "numberOfConnectionRetries": 0,

"delayBetweenRetries": 30, "maxConcurrentThreads": 1, "connectionTimeout": 30,

"port": { "mode": "AUTO", "min": 0, "max": 65535 }, "validateFileIntegrity": false,

"ASCIIFileExts": [ "TXT", "INF", "HTML", "HTM" ], "homeIP": "0.0.0.0",

"clearCommandChannel": false, "clearDataChannel": false, "transferEncoding":
"AutoDetect",

"timeStamp": { "preserveLocal": false, "preserveRemote": false } } } }, "links": {

"self": "/admin/v2/sites/76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles/

92e9f684-5b87-47d3-816b-19644e639ae2" } } }
```


POST PowerShell Sample

```
################################################

###POST Create New Connection Profile###

Write-Output " Create New Connection Profile"

Write-Output "-----------------------------"

$update =

'{

  "data": {

    "id": "",

    "type": "connectionProfile",

    "attributes": {

      "name": "PS REQUEST Create connection Profile",

      "description": "Connection Profile Details",
```

```
      "testPath": "\test",
      "connectionSettings": {
        "protocol": "FTPSAuthTLS",
        "host": "192.168.1.210",
        "port": 21,
        "user": "AFAR",
        "password": "",
        "autoLogin": true,
        "certSettings": {
          "certPath": "C:\\Users\\Administrator\\Desktop\\AFAR SSL\\SSL Cert User
AFAR.crt",
          "keyPath": "C:\\Users\\Administrator\\Desktop\\AFAR SSL\\SSL Cert User
AFAR.key",
          "passphrase": "xamYEctkRdBRCxu0F5XqoQ=="
        }
      }
    }
 }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 25
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/connection-Profiles" -
Method 'POST'
-Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/connection-profiles/{connectionProfileID}

> **NOTE:** Available as of EFT 8.1.0

- GET - Retrieves the details of a specified connection profile.
- PATCH - Updates the details of a specified connection profile.
- DELETE - Removes the specified connection profile.

Method & URL

```
GET https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles
```

GET Body Sample

```
### GET Details for specific connection profile####

###You can enter the Connection profile ID below or pass the value from a previous request###

##@ConnectionProfileID = 31334739-2f41-4561-9d27-22e17c9b9362

GET https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles/{{ConnectionProfileID}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Thu, 04 Aug 2022 16:11:35 GMT Location: /admin/v2/sites/

76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles/c9ea36ec-8a9e-440f-8c21-920eb3927732

Content-Type: application/vnd.api+json ETag: "A50CA65F" Content-Length: 1289

Cache-Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'

data:; Referrer-Policy: no-referrer

{ "data": { "id": "c9ea36ec-8a9e-440f-8c21-920eb3927732", "type": "connectionProfile", "attributes": {
```

```
"type": "Protocol", "name": "POST REQUEST Create connection Profile", "description":
"Connection Profile Details",

"connectionSettings": { "protocol": "FTPSAuthTLS", "user": "AFAR", "password":
"UpKUJq1sD4Yfb1Hz8ZFiRw==",

"autoLogin": true, "testPath": "\test", "host": "192.168.1.210", "port": 21,
"SSLCertificate": { "certPath": "",

"keyPath": "", "passphrase": "UpKUJq1sD4Yfb1Hz8ZFiRw==" }, "trustedPubKey": "", "proxy":
{ "use": false,

"type": "FTP", "hostName": "", "username": "", "password": "UpKUJq1sD4Yfb1Hz8ZFiRw==",
"port": 21,

"subType": 0, "separator": "@", "customCommands": [] }, "socks": { "use": false, "type":
"None",

"hostName": "", "port": 1080, "auth": false, "username": "", "password":
"UpKUJq1sD4Yfb1Hz8ZFiRw==" },

"advanced": { "numberOfConnectionRetries": 0, "delayBetweenRetries": 30,
"maxConcurrentThreads": 1,

"connectionTimeout": 30, "port": { "mode": "AUTO", "min": 0, "max": 65535 },
"validateFileIntegrity": false,

"ASCIIFileExts": [ "TXT", "INF", "HTML", "HTM" ], "homeIP": "0.0.0.0",
"clearCommandChannel": false,

"clearDataChannel": false, "transferEncoding": "AutoDetect", "timeStamp": {
"preserveLocal": false,

"preserveRemote": false } } } }, "links": { "self": "/admin/v2/sites/

76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles/c9ea36ec-8a9e-440f-8c21-
920eb3927732" } }

}
```


GET PowerShell Sample


```
HTTP/1.1 200 OK Date: Thu, 04 Aug 2022 16:11:35 GMT Location: /admin/v2/sites/

76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles/c9ea36ec-8a9e-440f-8c21-
920eb3927732

Content-Type: application/vnd.api+json ETag: "A50CA65F" Content-Length: 1289 Cache-
Control: no-cache,

no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection:
1; mode=block

Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;

Referrer-Policy: no-referrer {

"data": { "id": "c9ea36ec-8a9e-440f-8c21-920eb3927732", "type": "connectionProfile",
"attributes": {

"type": "Protocol", "name": "POST REQUEST Create connection Profile", "description":

"Connection Profile Details", "connectionSettings": { "protocol": "FTPSAuthTLS", "user":
"AFAR",
```

```
"password": "UpKUJq1sD4Yfb1Hz8ZFiRw==", "autoLogin": true, "testPath": "\test", "host":
"192.168.1.210",

"port": 21, "SSLCertificate": { "certPath": "", "keyPath": "", "passphrase":
"UpKUJq1sD4Yfb1Hz8ZFiRw==" },

"trustedPubKey": "", "proxy": { "use": false, "type": "FTP", "hostName": "", "username":
"",

"password": "UpKUJq1sD4Yfb1Hz8ZFiRw==", "port": 21, "subType": 0, "separator": "@",
"customCommands": [] },

"socks": { "use": false, "type": "None", "hostName": "", "port": 1080, "auth": false,
"username": "",

"password": "UpKUJq1sD4Yfb1Hz8ZFiRw==" }, "advanced": { "numberOfConnectionRetries": 0,

"delayBetweenRetries": 30, "maxConcurrentThreads": 1, "connectionTimeout": 30, "port": {
"mode": "AUTO",

"min": 0, "max": 65535 }, "validateFileIntegrity": false, "ASCIIFileExts": [ "TXT",
"INF", "HTML", "HTM" ],

"homeIP": "0.0.0.0", "clearCommandChannel": false, "clearDataChannel": false,
"transferEncoding": "AutoDetect",

"timeStamp": { "preserveLocal": false, "preserveRemote": false } } } }, "links": {
"self":

"/admin/v2/sites/76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles/c9ea36ec-8a9e-
440f-8c21-920eb3927732" } }

}
```


Method & URL

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/connection-
Profiles/{[ConnectionProfileID}}
```

PATCH Body Sample

```
### Update a Connection Profile ####

###You can enter the Connection profile ID below or pass the value from a previous
request###

##@ConnectionProfileID = 31334739-2f41-4561-9d27-22e17c9b9362

PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles/
{{ConnectionProfileID}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
      "type": "connectionProfile",
      "attributes": {
```

```
        "name": "Patch Connection Profile",
        "description": "Patch Connection Profile",
        "testPath": "/",
        "connectionSettings": {
          "protocol": "FTPSAuthTLS",
          "host": "192.168.1.210",
          "port": 21,
          "user": "AFAR",
          "password": "pass",
          "autoLogin": false
          }
        }
      }
}
```

PATCH Response Body Sample

```
HTTP/1.1 200 OK Date: Thu, 04 Aug 2022 18:33:38 GMT Location: /admin/v2/sites/
76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles/c9ea36ec-8a9e-440f-8c21-
920eb3927732
Content-Type: application/vnd.api+json ETag: "624A277A" Content-Length: 1408
Cache-Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options:
nosniff
X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self' 'unsafe-
inline'
'unsafe-eval' data:; Referrer-Policy: no-referrer { "data": { "id": "c9ea36ec-8a9e-440f-
8c21-920eb3927732",
"type": "connectionProfile", "attributes": { "type": "Protocol", "name": "Patch
Connection Profile",
"description": "Patch Connection Profile", "connectionSettings": { "protocol":
"FTPSAuthTLS",
"user": "AFAR", "password": "wweZ1iVXRYBbX80z2T3JHg==", "autoLogin": false, "testPath":
"/",
"host": "192.168.1.210", "port": 21, "SSLCertificate": { "certPath":
"C:\\Users\\administrator.TEST\\Desktop\\AFAR SSL\\SSL Cert User AFAR.crt", "keyPath":
"C:\\Users\\administrator.TEST\\Desktop\\AFAR SSL\\SSL Cert User AFAR.key",
"passphrase": "xamYEctkRdBRCxu0F5XqoQ==" }, "trustedPubKey": "", "proxy": { "use":
false,
"type": "FTP", "hostName": "", "username": "", "password": "UpKUJq1sD4Yfb1Hz8ZFiRw==",
```

```
"port": 21, "subType": 0, "separator": "@", "customCommands": [] }, "socks": { "use":
false,

"type": "None", "hostName": "", "port": 1080, "auth": false, "username": "",

"password": "UpKUJq1sD4Yfb1Hz8ZFiRw==" }, "advanced": { "numberOfConnectionRetries": 0,

"delayBetweenRetries": 30, "maxConcurrentThreads": 1, "connectionTimeout": 30,

"port": { "mode": "AUTO", "min": 0, "max": 65535 }, "validateFileIntegrity": false,

"ASCIIFileExts": [ "TXT", "INF", "HTML", "HTM" ], "homeIP": "0.0.0.0",
"clearCommandChannel": false,

"clearDataChannel": false, "transferEncoding": "UTF8", "timeStamp": { "preserveLocal":
false,

"preserveRemote": false } } } }, "links": { "self": "/admin/v2/sites/

76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles/c9ea36ec-8a9e-440f-8c21-
920eb3927732" } }

}
```

Endpoint: /experimental/site/templates/{templateName}

Returns the contents of the specified site template

Note: Available as of EFT 8.1.0

- GET
- PATCH

Method & URL

```
GET https://{{host}}/admin/v2/sites/{{Siteid}}/templates/{templateName}
```

GET Body Sample

```
#GET Site Templates -- ##

GET https://{{host}}/admin/v2/sites/{{Siteid}}/templates/WorkspacesAdminAddedParticipantMsg.html HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 13:01:21 GMT Content-Type: application/vnd.api+json

Content-Length: 370 Cache-Control: no-cache, no-store, must-revalidate Expires: -1

X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;

Referrer-Policy: no-referrer { "data": "<html>\r\n<body>\r\n <p>Hello %USER.LOGIN%,</p>\r\n

<p>The following <b>Enhanced File Transfer</b> Workspace has been shared with you:

%FOLDER_NAME% (owner: %WS_OWNER_NAME%).</p>\r\n <p>Please use the following URL to

access this Workspace:</p>\r\n <a href=\"%LINK%\">%LINK%</a><br/><br/>\r\n \r\n

%WS_MESSAGE%<br/><br/>\r\n <hr/>\r\n</body>\r\n</html>" }
```

GET PowerShell Sample

```
####################################
#GET Site Template Details -- ##
Write-Output "GET Site Template Detail"
Write-Output "------------------------------"
#$siteID = "Enter site ID"
#$TemplateName= "WorkspacesAdminAddedParticipantMsg.html"
$TemplateDetails = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/templates/
WorkspacesAdminAddedParticipantMsg.html"
-Method 'GET' -Headers $authHeader
Write-Output $TemplateDetails | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH https://{{host}}/admin/v2/sites/
{{Siteid}}/templates/WorkspacesAdminAddedParticipantMsg.html
```

PATCH Body Sample

```
#Modify Site Template - Will append the site name to the file name should only be used
for this site ##
PATCH https://{{host}}/admin/v2/sites/
{{Siteid}}/templates/WorkspacesAdminAddedParticipantMsg.html HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": "<html>\r\n<body>\r\n  <p>Update Template Example
%USER.LOGIN%,</p>\r\n  <p>The following
  <b>Enhanced File Transfer</b> Workspace has been shared with you: %FOLDER_NAME%
(owner: %WS_OWNER_NAME%).
  </p>\r\n  <p>Please use the following URL to access this Workspace:</p>\r\n  <a
href=\"%LINK%\">%LINK%</a>
  <br/><br/>\r\n  \r\n  %WS_MESSAGE%<br/><br/>\r\n  <hr/>\r\n</body>\r\n</html>"
}


####
```

PATCH Response Body Sample

```
HTTP/1.1 204 No Content Date: Fri, 05 Aug 2022 13:48:49 GMT Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

PATCH PowerShell Sample

```
####Added 8/4/2022
### Update Content of Template###
### Modify Site Template - Will append the site name to the file name should only be
used for this site  ###
Write-Output "PATCH Site Connection Profile"
Write-Output "-----------------------------"
$update =
'{
  "data": "<html>\r\n<body>\r\n  <p>PS1. Update Template Example %USER.LOGIN%,</p>\r\n
  <p>The following <b>Enhanced File Transfer</b> Workspace has been shared with you:
%FOLDER_NAME%
  (owner: %WS_OWNER_NAME%).</p>\r\n  <p>Please use the following URL to access this
  Workspace:</p>\r\n  <a href=\"%LINK%\">%LINK%</a><br/><br/>\r\n  \r\n  %WS_
MESSAGE%<br/>
  <br/>\r\n  <hr/>\r\n</body>\r\n</html>"
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$TemplateDetails = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/templates/
WorkspacesAdminAddedParticipantMsg.html"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint:/sites/{siteID}/dmz

Note: Available as of EFT 8.1.0

(GET) Returns DMZ gateway settings from specified site and (PATCH) updates DMZ gateway settings

- GET
- PATCH

Method & URL

```
GET https://{{host}}/admin/v2/sites/{{Siteid}}/dmz
```

GET Body Sample

```
### GET SITE DMZ INFO ###

GET https://{{host}}/admin/v2/sites/{{Siteid}}/dmz HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample


```
{"data":{"type":"DMZGateway","attributes":{"enabled":false,"hosts":
[],"port":44500,"securePNC":{

"enabled":false,"publicKeyPath":""},"ftp":{"enabled":false,"port":21},"ftpsExpl":
{"enabled":false,

"port":21},"ftpsImpl":{"enabled":false,"port":990},"sftp":
{"enabled":false,"port":22},"http":{

"enabled":false,"port":80},"https":{"enabled":false,"port":443},"internalDomain":
{"HTTPDomain":"",

"emailDomainPatterns":"","allowADorLDAPAuth":true,"isExclusiveADorLDAP":false,

"isRequired2FAforInternalUsers":false,"SSLCertificate":
{"certPath":"","keyPath":"","passphrase":

"UpKUJq1sD4Yfb1Hz8ZFiRw=="},"pasv":
{"enabled":false,"listenIP":"0.0.0.0","portMin":28000,

"portMax":30000},"remoteAdmin":{"enabled":false,"port":1100},"acceleration":
{"enabled":false,

"port":8443}},"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-
477c08f0abca/dmz"}}}
```

GET PowerShell Sample

Method & URL

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/dmz
```

PATCH Body Sample

```
### PATCH (UPDATE) DMZ INFO ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/dmz HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "DMZGateway",
    "attributes": {
      "hosts":
      [
        "10.91.160.102"
      ],
      "port":"44500",
      "enabled": true,
      "ftpEnabled": false,
      "ftpsEnabled": true,
      "ftpsExpEnabled": true,
      "sftpEnabled": false,
      "ftpPort": 21,
      "ftpsPort": 990,
      "httpsEnabled": true,
      "adminEnabled": true,
      "adminPort": 1100
    }
  }
}
###
```

PATCH Response Body Sample


```
{"data":{"type":"DMZGateway","attributes":{"enabled":true,"hosts":
["10.91.160.102"],"port":44500,

"securePNC":{"enabled":false,"publicKeyPath":""},"ftp":
{"enabled":false,"port":21},"ftpsExpl":

{"enabled":false,"port":21},"ftpsImpl":{"enabled":false,"port":990},"sftp":{

"enabled":false,"port":22},"http":{"enabled":false,"port":80},"https":{

"enabled":false,"port":443},"internalDomain":{"HTTPDomain":"","emailDomainPatterns":"",

"allowADorLDAPAuth":true,"isExclusiveADorLDAP":false,"isRequired2FAforInternalUsers":fal
se,

"SSLCertificate":{"certPath":"","keyPath":"","passphrase":"UpKUJq1sD4Yfb1Hz8ZFiRw=="}},

"pasv":{"enabled":false,"listenIP":"0.0.0.0","portMin":28000,"portMax":30000},

"remoteAdmin":{"enabled":false,"port":1100},"acceleration":
{"enabled":false,"port":8443}},

"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-477c08f0abca/dmz"}}}
```


PATCH PowerShell Sample

```
##Patch SITE DMZ settings

Write-Output "Site DMZ PATCH"

Write-Output "-----"

$update =

'{
  "data": {
    "type": "DMZGateway",
    "attributes": {
      "hosts":
      [
        "10.91.160.102"
      ],
      "port":"44500",
      "enabled": true,
      "ftpEnabled": false,
      "ftpsEnabled": true,
      "ftpsExpEnabled": true,
      "sftpEnabled": false,
      "ftpPort": 21,
      "ftpsPort": 990,
```

```
      "httpsEnabled": true,
      "adminEnabled": true,
      "adminPort": 1100
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchDMZReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/dmz"
-Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $patchDMZReturn | ConvertTo-Json
```

Security REST API

The endpoints described in this section are related to algorithms and ciphers.

- Endpoint: /lists/security/ssh/algorithms
- Endpoint: /lists/security/tls/algorithms
- Endpoint: /lists/security/tls/ciphers/{cipherString}

Endpoint: /lists/security/ssh/algorithms

Returns a list of ssh algorithms

- GET

Method & URL

```
GET https://[server URL]:
[port]/admin/v2/lists/security/ssh/algorithms
```

GET Body Sample

```
###
##Get Server SSH Security Settings
GET https://{{host}}/admin/v2/lists/security/ssh/algorithms HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "attributes": { "algorithms": { "ciphers": [ "aes256-gcm@openssh.com",
"aes256-ctr",
"aes256-cbc", "rijndael-cbc@lysator.liu.se", "twofish256-cbc", "twofish-cbc", "aes192-
ctr",
"aes192-cbc", "aes128-gcm@openssh.com", "aes128-ctr", "aes128-cbc", "twofish128-cbc",
```

GET PowerShell Sample

```
###
#GET SSH ALOGRITHMS
Write-Output "Get EFT SSH ALGORITHMS"
$serverNodeID = "DTY2019WinServe"

Write-Output "Server Node: $serverNodeID"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/lists/security/ssh/algorithms"
-Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Endpoint: /lists/security/tls/algorithms

Returns a list of tls algorithms

- GET

Method & URL

```
GET https://[server URL]:
[port]/admin/v2/lists/security/tls/algorithms
```

GET Body Sample

```
###
##Get Server TLS Security Settings
GET https://{{host}}/admin/v2/lists/security/tls/algorithms HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "attributes": { "resultingCipherList": [ "ECDHE-ECDSA-AES256-GCM-SHA384",
"ECDHE-RSA-AES256-GCM-SHA384", "DHE-RSA-AES256-GCM-SHA384", "ECDHE-ECDSA-CHACHA20-
POLY1305",
"ECDHE-RSA-CHACHA20-POLY1305", "DHE-RSA-CHACHA20-POLY1305", "ECDHE-ECDSA-AES128-GCM-
SHA256",
"ECDHE-RSA-AES128-GCM-SHA256", "DHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-SHA384",
"ECDHE-RSA-AES256-SHA384", "DHE-RSA-AES256-SHA256", "ECDHE-ECDSA-AES128-SHA256",
"ECDHE-RSA-AES128-SHA256",
```

GET PowerShell Sample

```
###
#GET TLS ALOGRITHMS
Write-Output "Get EFT TLS ALGORITHMS"
$serverNodeID = "DTY2019WinServe"

Write-Output "Server Node: $serverNodeID"
Write-Output "-----"
```

```
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/lists/security/tls/algorithms"
-Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Endpoint: /lists/security/tls/ciphers/{cipherString}

Returns a list of resulting ciphers

- GET

Method & URL

```
GET https://[server URL]:
[port]/admin/v2/lists/security/tls/ciphers/{cipherString}
```

GET Body Sample

```
###
##Get Server TLS Ciphers Settings
GET https://{{host}}/admin/v2/lists/security/tls/ciphers/"aes-ctr" HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
#
```

GET Response Body Sample

```
{ "data": { "attributes": { "resultingCipherList": [ "ECDHE-ECDSA-AES256-GCM-SHA384",
"ECDHE-RSA-AES256-GCM-SHA384", "DHE-RSA-AES256-GCM-SHA384", "ECDHE-ECDSA-CHACHA20-
POLY1305",
"ECDHE-RSA-CHACHA20-POLY1305", "DHE-RSA-CHACHA20-POLY1305", "ECDHE-ECDSA-AES128-GCM-
SHA256",
"ECDHE-RSA-AES128-GCM-SHA256", "DHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-SHA384",
"ECDHE-RSA-AES256-SHA384", "DHE-RSA-AES256-SHA256", "ECDHE-ECDSA-AES128-SHA256",
"ECDHE-RSA-AES128-SHA256",
```

GET PowerShell Sample

```
###
#GET TLS CIPHERS
Write-Output "Get EFT TLS CIPHERS"
$serverNodeID = "DTY2019WinServe"
$cipherId = "aes-ctr"
```

```
Write-Output "Server Node: $serverNodeID"

Write-Output "-----""

$serverAdminDetails = Invoke-RestMethod -Uri
"$baseURL/v2/lists/security/tls/ciphers/$cipherID

-Method 'GET' -Headers $authHeader

Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Login/Logout REST API

Endpoint: /logout

Logs out of current session.

- POST

Method & URL

```
POST https://[server URL]:[port]/admin/v2/logout
```

POST Body Sample

```
POST https://{{host}}/admin/v2/logout HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

POST Response Body Sample

```
HTTP/1.1 200 OK Date: Wed, 10 Aug 2022 20:10:28 GMT Content-Length: 0 Set-Cookie:
websessionid=xxxxxx;
expires=Tuesday, 10-Aug-21 20:10:28 GMT; path=/; secure; HttpOnly; SameSite=Strict
Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'
data:; Referrer-Policy: no-referrer
```

POST PowerShell Sample

```
# POST - logout
$auth = Invoke-RestMethod -Uri "$baseURL/v2/logout"
-Method 'POST' -Body $authBody -Headers $authHeader
#
```

Keep-Alive REST API

Endpoint: /keep-alive

> **NOTE:** This endpoint works in v8.1, but not in v8.2 and later

Extends current session.

- HEAD

Method & URL

```
HEAD https://[server URL]:[port]/admin/v2/keep-alive
```

HEAD Body Sample

```
##Get Server keep alive
HEAD https://{{host}}/admin/v2/keep-alive HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

HEAD Response Body Sample

```
HTTP/1.1 200 OK Date: Mon, 21 Feb 2022 22:17:46 GMT Content-Length: 0 Cache-Control: no-
cache,
no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection:
1;
mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;
Referrer-Policy: no-referrer
```

HEAD PowerShell Sample

```
# keep-alive
Write-Output "Keep Alive"
Write-Output "----"
$keepAlive = Invoke-RestMethod -Uri "$baseURL/v2/keep-alive"
-Method 'HEAD' -Headers $authHeader
```

Users REST API

The endpoints described in this section are part of /sites/siteId/ related to users.

- Endpoint: /sites/{siteId}/users
- Endpoint: /sites/{siteid}/users/{userid}
- Endpoint: /sites/{siteid}/users/{userid}/as2inbound
- Endpoint: /sites/{siteid}/users/{userid}/as2outbound
- Endpoint: /sites/{siteid}/users/{userid}/counters

Endpoint: /sites/{siteId}/users

Returns a list of users for specific site, create user(s) for a specific site.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/users
```

GET Body Sample

```
### GET SITE USERS ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": [ { "attributes": { "accountEnabled": "inherit", "agreementToTermsOfService":
"unknown", "as2": { "inbound": { "enabled": "inherit" }, "outbound": { "enabled":
"inherit" } },
"changePassword": { "enabled": "inherit", "value": {
"changeAdminProvidedPasswordUponFirstUse":
"inherit", "mustChangePassword": false, "passwordExpiration": { "enabled": true,
"value": {
"maxAgeDays": 90, "emailUpon": true,
```

GET PowerShell Sample

```
# get sites
Write-Output "Site"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites"
-Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
foreach ($site in $siteList.data)
```

```
{
    Write-Output ("Site  $($site.id): $($site.attributes.name)")
}

$siteID = $siteList.data[0].id

# get users
Write-Output "Users"
Write-Output "-----"
$userList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users"
-Method 'GET' -Headers $authHeader
Write-Output $userList | ConvertTo-Json
foreach ($user in $userList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/ sites/{siteId}/users
```

POST Body Sample

```
### ADD SITE USER ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "user",
    "attributes": {
      "loginName": "TestUser1",
      "password": {
        "type": "Disabled",
        "value": "Alaska12#"
      },
      "accountEnabled": "inherit",
```

```
"expiration": {
  "enabled": false,
  "value": {
    "date": {}
  }
},
"personal": {
  "name": "Test User",
  "description": null,
  "email": null,
  "DUNS": null,
  "phone": null,
  "mobile": null,
  "pager": null,
  "fax": null,
  "company": null,
  "partnerId": null,
  "custom1": null,
  "custom2": null,
  "custom3": null,
  "comments": null
},
"isEuDataSubject": "unknown",
"consentToPrivacyPolicy": "unknown",
"agreementToTermsOfService": "unknown",
"homeFolder": {
  "enabled": "yes",
  "value": {
    "path": null
  }
},
"hasHomeFolderAsRoot": "inherit",
"externalAuthentication": "inherit",
"ftp": {
  "enabled": "inherit",
  "value": {
    "enableFxp": "inherit",
```

```
      "enableNoop": "inherit",
      "enableComb": "inherit",
      "enableXcrc": "inherit",
      "enableZlib": "inherit",
      "banner": {
        "message": "",
        "usage": "useDefault"
      }
    }
  },
  "ftps": {
    "enabled": "inherit"
  },
  "sftp": {
    "enabled": "inherit",
    "value": {
      "authenticationType": "inherit"
    }
  },
  "http": {
    "enableHttp": "inherit",
    "enableHttps": "inherit",
    "enableWtc": "inherit",
    "enableShareFolder": "inherit",
    "enableSendMessage": "inherit"
  },
  "ssl": {
    "authenticationType": "inherit"
  },
  "as2": {
    "inbound": {
      "enabled": "inherit"
    },
    "outbound": {
      "enabled": "inherit"
    }
  },
```

```
  "transferSpeedLimit": {
    "enabled": "inherit",
    "value": {
      "maxKbps": 0
    }
  },
  "connectionTimeout": {
    "enabled": "inherit",
    "value": {
      "maxSec": 0
    }
  },
  "totalConnectionsLimit": {
    "enabled": "inherit",
    "value": {
      "maxNumber": 0
    }
  },
  "connectionsFromSameIpLimit": {
    "enabled": "inherit",
    "value": {
      "maxNumber": 0
    }
  },
  "uploadsPerSessionLimit": {
    "enabled": "inherit",
    "value": {
      "maxNumber": 0
    }
  },
  "downloadsPerSessionLimit": {
    "enabled": "inherit",
    "value": {
      "maxNumber": 0
    }
  },
  "uploadSizeLimit": {
```

```
      "enabled": "inherit",
      "value": {
        "maxKBytes": 0
      }
    },
    "downloadSizeLimit": {
      "enabled": "inherit",
      "value": {
        "maxKBytes": 0
      }
    },
    "ipAccessLimit": {
      "enabled": "inherit",
      "value": {
        "rules": [],
        "defaultRule": "allowAccess"
      }
    },
    "invalidLoginLimit": {
      "enabled": "inherit",
      "value": {
        "maxCount": 90,
        "periodMin": 5,
        "action": "lock",
        "actionDurationMin": 30
      }
    },
    "passwordComplexity": {
      "enabled": "inherit",
      "value": {
        "minLength": 8,
        "characterCategories": {
          "enabled": true,
          "value": {
            "characterCount": 4,
            "upperCaseRequired": true,
            "lowerCaseRequired": true,
```

```
            "numericRequired": true,
            "nonAlphaNumericRequired": true,
            "non7bitAsciiRequired": true
          }
        },
        "usernameCharLimit": {
          "enabled": true,
          "value": {
            "minDisallowed": 3
          }
        },
        "repeatingCharLimit": {
          "enabled": true,
          "value": {
            "minDisallowed": 3
          }
        },
        "forbiddenDictionary": {
          "enabled": true,
          "value": {
            "dictionaryFilePath": "Dictionary.txt",
            "noBackwardsWord": false
          }
        }
      }
    },
    "changePassword": {
      "enabled": "inherit",
      "value": {
        "changeAdminProvidedPasswordUponFirstUse": "inherit",
        "mustChangePassword": false,
        "passwordExpiration": {
          "enabled": true,
          "value": {
            "maxAgeDays": 90,
            "emailUpon": true,
            "remindPrior": {
```

```
            "enabled": false,
            "value": {
              "daysBefore": 5,
              "emailUser": true
            }
          }
        }
      }
    }
  },
  "passwordHistory": {
    "enabled": "inherit",
    "value": {
      "historyDepth": 4
    }
  },
  "inactivityLimit": {
    "enabled": "inherit",
    "value": {
      "days": 90,
      "action": "remove"
    }
  }
},
"relationships": {
  "userTemplate": {
    "data": {
      "type": "userTemplate",
      "id": "65189354-3ab5-42b3-9281-37939abd8389"
    }
  },
  "permissionGroups": {
    "data": [
      {
        "type": "permissionGroup",
        "id": "a0db9377-92a3-4a38-8c0f-09f268d78ff1"
      }
```

```
        ]
      },
      "sslCertificate": {
        "data": null
      },
      "sshKeys": {
        "data": []
      }
    }
  }
}
```

POST Response Body Sample

```
"data": { "attributes": { "accountEnabled": "inherit", "agreementToTermsOfService":
"unknown",
"as2": { "inbound": { "enabled": "inherit" }, "outbound": { "enabled": "inherit" } },
"changePassword": { "enabled": "inherit", "value": {
"changeAdminProvidedPasswordUponFirstUse":
"inherit", "mustChangePassword": false, "passwordExpiration": { "enabled": true,
"value": {
"maxAgeDays": 90, "emailUpon": true, "remindPrior": { "enabled": false, "value": {
"daysBefore": 5, "emailUser": true } } } } } }, "connectionTimeout": { "enabled":
"inherit",
"value": { "maxSec": 0 } },
```

POST PowerShell Sample

```
Write-Output "Add User POST"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "user",
    "attributes": {
      "loginName": "TestUser2",
      "password": {
```

```
    "type": "Disabled",
    "value": "Alaska12#"
  },
  "accountEnabled": "inherit",
  "expiration": {
    "enabled": false,
    "value": {
      "date": {}
    }
  },
  "personal": {
    "name": "Test User",
    "description": null,
    "email": null,
    "DUNS": null,
    "phone": null,
    "mobile": null,
    "pager": null,
    "fax": null,
    "company": null,
    "partnerId": null,
    "custom1": null,
    "custom2": null,
    "custom3": null,
    "comments": null
  },
  "isEuDataSubject": "unknown",
  "consentToPrivacyPolicy": "unknown",
  "agreementToTermsOfService": "unknown",
  "homeFolder": {
    "enabled": "yes",
    "value": {
      "path": null
    }
  },
  "hasHomeFolderAsRoot": "inherit",
  "externalAuthentication": "inherit",
```

```
"ftp": {
  "enabled": "inherit",
  "value": {
    "enableFxp": "inherit",
    "enableNoop": "inherit",
    "enableComb": "inherit",
    "enableXcrc": "inherit",
    "enableZlib": "inherit",
    "banner": {
      "message": "",
      "usage": "useDefault"
    }
  }
},
"ftps": {
  "enabled": "inherit"
},
"sftp": {
  "enabled": "inherit",
  "value": {
    "authenticationType": "inherit"
  }
},
"http": {
  "enableHttp": "inherit",
  "enableHttps": "inherit",
  "enableWtc": "inherit",
  "enableShareFolder": "inherit",
  "enableSendMessage": "inherit"
},
"ssl": {
  "authenticationType": "inherit"
},
"as2": {
  "inbound": {
    "enabled": "inherit"
  },
```

```
    "outbound": {
      "enabled": "inherit"
    }
  },
  "transferSpeedLimit": {
    "enabled": "inherit",
    "value": {
      "maxKbps": 0
    }
  },
  "connectionTimeout": {
    "enabled": "inherit",
    "value": {
      "maxSec": 0
    }
  },
  "totalConnectionsLimit": {
    "enabled": "inherit",
    "value": {
      "maxNumber": 0
    }
  },
  "connectionsFromSameIpLimit": {
    "enabled": "inherit",
    "value": {
      "maxNumber": 0
    }
  },
  "uploadsPerSessionLimit": {
    "enabled": "inherit",
    "value": {
      "maxNumber": 0
    }
  },
  "downloadsPerSessionLimit": {
    "enabled": "inherit",
    "value": {
```

```
      "maxNumber": 0
    }
  },
  "uploadSizeLimit": {
    "enabled": "inherit",
    "value": {
      "maxKBytes": 0
    }
  },
  "downloadSizeLimit": {
    "enabled": "inherit",
    "value": {
      "maxKBytes": 0
    }
  },
  "ipAccessLimit": {
    "enabled": "inherit",
    "value": {
      "rules": [],
      "defaultRule": "allowAccess"
    }
  },
  "invalidLoginLimit": {
    "enabled": "inherit",
    "value": {
      "maxCount": 90,
      "periodMin": 5,
      "action": "lock",
      "actionDurationMin": 30
    }
  },
  "passwordComplexity": {
    "enabled": "inherit",
    "value": {
      "minLength": 8,
      "characterCategories": {
        "enabled": true,
```

```
        "value": {
          "characterCount": 4,
          "upperCaseRequired": true,
          "lowerCaseRequired": true,
          "numericRequired": true,
          "nonAlphaNumericRequired": true,
          "non7bitAsciiRequired": true
        }
      },
      "usernameCharLimit": {
        "enabled": true,
        "value": {
          "minDisallowed": 3
        }
      },
      "repeatingCharLimit": {
        "enabled": true,
        "value": {
          "minDisallowed": 3
        }
      },
      "forbiddenDictionary": {
        "enabled": true,
        "value": {
          "dictionaryFilePath": "Dictionary.txt",
          "noBackwardsWord": false
        }
      }
    }
  },
  "changePassword": {
    "enabled": "inherit",
    "value": {
      "changeAdminProvidedPasswordUponFirstUse": "inherit",
      "mustChangePassword": false,
      "passwordExpiration": {
        "enabled": true,
```

```
          "value": {
            "maxAgeDays": 90,
            "emailUpon": true,
            "remindPrior": {
              "enabled": false,
              "value": {
                "daysBefore": 5,
                "emailUser": true
              }
            }
          }
        }
      }
    },
    "passwordHistory": {
      "enabled": "inherit",
      "value": {
        "historyDepth": 4
      }
    },
    "inactivityLimit": {
      "enabled": "inherit",
      "value": {
        "days": 90,
        "action": "remove"
      }
    }
  },
  "relationships": {
    "userTemplate": {
      "data": {
        "type": "userTemplate",
        "id": "65189354-3ab5-42b3-9281-37939abd8389"
      }
    },
    "permissionGroups": {
      "data": [
```

```
          {
            "type": "permissionGroup",
            "id": "a0db9377-92a3-4a38-8c0f-09f268d78ff1"
          }
        ]
      },
      "sslCertificate": {
        "data": null
      },
      "sshKeys": {
        "data": []
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$PostReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users"
-Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteid}/users/{userid}

Returns, updates, and deletes user account details.

- GET
- PATCH
- DELETE
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/users/
{userid}
```

GET Body Sample

```
### GET SITE SPECIFIC USER ###
# @name usersList
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###

@Usersid = {{usersList.response.body.$.data[0].id}}
###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": { "attributes": { "accountEnabled": "inherit", "agreementToTermsOfService":
"unknown", "as2": {
"inbound": { "enabled": "inherit" }, "outbound": { "enabled": "inherit" } },
"changePassword": {
"enabled": "inherit", "value": { "changeAdminProvidedPasswordUponFirstUse": "inherit",
"mustChangePassword": false, "passwordExpiration": { "enabled": true, "value": {
"maxAgeDays": 90,
"emailUpon": true, "remindPrior": { "enabled": false, "value": { "daysBefore": 5,
"emailUser": true
```

GET PowerShell Sample

```
# get a specific users information
Write-Output "Users"
Write-Output "-----"
$userList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users"
-Method 'GET' -Headers $authHeader
Write-Output $userList | ConvertTo-Json
foreach ($user in $userList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}

$userid = $userList.data[0].id

# get user’s data
Write-Output "Users"
Write-Output "-----"
$userList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users/$userid"
-Method 'GET' -Headers $authHeader
Write-Output $userList | ConvertTo-Json
foreach ($user in $userList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/users/{userid}/
```

PATCH Body Sample

```
@Usersid = {{usersList.response.body.$.data[0].id}}
###
### UPDATE A USERS PERSONAL INFORMATION ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

```
{
  "data": {
    "type": "user",
    "attributes": {
      "personal": {
        "name": "MR JONES",
        "description": “MANAGER",
        "email": "user@example.com",
        "duns": "",
        "phone": "",
        "mobile": "2107221301",
        "pager": "",
        "fax": "",
        "company": "",
        "partnerId": "",
        "custom1": "1234",
        "custom2": "5678",
        "custom3": "abcd",
        "comments": "Does this work?"
      },
      "isEuDataSubject": "yes",
      "consentToPrivacyPolicy": "grantedExplicit",
      "agreementToTermsOfService": "agreedExplicit"
     }
  }
}
```

PATCH Response Body Sample

```
{ "data": { "attributes": { "accountEnabled": "inherit", "agreementToTermsOfService":
"agreedExplicit",

"as2": { "inbound": { "enabled": "inherit" }, "outbound": { "enabled": "inherit" } },
"changePassword": {

"enabled": "inherit", "value": { "changeAdminProvidedPasswordUponFirstUse": "inherit",

"mustChangePassword": false, "passwordExpiration": { "enabled": true, "value": {
"maxAgeDays": 90,
```

```
"emailUpon": true, "remindPrior": { "enabled": false, "value": { "daysBefore": 5,
"emailUser": true } } } } } },
"connectionTimeout": { "enabled": "inherit", "value": { "maxSec": 0 }
```

PATCH PowerShell Sample

```
##UPDATE USERS
Write-Output "Update user data"
Write-Output "-----"
$update =
'{
    "data": {
       "type": "user",
       "attributes": {
       "accountEnabled": "no"

       }
      }

}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$PatchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users/$userid"
-Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/
{siteId}/users/{userid}/
```

DELETE Body Sample

```
### REMOVE THE USER ### (userOnly, userAndHomeFolder)
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
```

```
    "parameters": {
        "scope": "userAndHomeFolder"
    }
}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Fri, 04 Feb 2022 21:00:36 GMT Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
$update =
'{
    "parameters": {
        "scope": "userAndHomeFolder"
    }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
# delete
Write-Output "Delete User"
Write-Output "-----"
$deleteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users/$userid"
-Method 'DELETE' -Headers $authHeader -Body $update
Write-Output $deleteList | ConvertTo-Json
foreach ($user in $deletList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /rpc/sites/{siteid}/users/{userid}

Returns, updates, and deletes user account details.

- POST

Method & URL

```
POST https://[server URL]:[port]/admin/v2/rpc/sites/
{siteId}/users/{userid}/
```

POST Body Sample

```
@Usersid = {{usersList.response.body.$.data[0].id}}

###
#### USER  OPERATION (KICK, RESETPASSWORD, UNLOCK) ####

POST https://{{host}}/admin/v2/rpc/sites/{{Siteid}}/users/{{Usersid}}/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data": {
        "type": "userOperation",
        "id": "0",
        "attributes": {
            "operation": "resetPassword"
        }
    }
}
```

POST Response Body Sample

```
{
  "data": {
    "type": "userOperation",
    "id": "0",
    "attributes": {
```

```
      "status": "success"
    }
  }
}
```

POST PowerShell Sample

```
##############################################################################################
################
$userid = $userList.data[0].id


Write-Output "Update user data - Reset Password"
Write-Output "-----"
$update =
'{
    "data": {
       "type": "userOperation",
       "id": "0",
       "attributes": {
       "operation": "resetPassword"


       }
      }


}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$PatchReturn = Invoke-RestMethod -Uri "$baseURL/v2/rpc/sites/$siteID/users/$userid" -
Method 'POST' -Headers $authHeader -Body $update


###
```

Endpoint: /sites/{siteid}/users/{userid}/as2inbound

Returns and updates user inbound AS2 parameters

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/as2inbound
```

GET Body Sample

```
# @name usersList
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###

@Usersid = {{usersList.response.body.$.data[0].id}}
###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}/as2inbound HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": { "attributes": { }, "relationships": { "transactionFailedCommand": { "data": null },
"transactionSuccessCommand": { "data": null } }, "type": "AS2Inbound" } }
```

GET PowerShell Sample

```
$userid = $userList.data[0].id

# get users
```

```
Write-Output "Specific User AS2inbound information"
Write-Output "-----"
$userList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users/$userid/as2inbound"
-Method 'GET' -Headers $authHeader
Write-Output $userList | ConvertTo-Json
foreach ($user in $userList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/users/
{userid}/as2inbound
```

PATCH Body Sample

```
###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}/as2inbound HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "AS2Inbound",
    "attributes": {
      "myId": "AS2_1",
      "partnerId": "AS2_2"
    }
  }
}
```

PATCH Response Body Sample

```
{
  "data": {
    "attributes": {
      "allowedEncryptionAlgorithms": [
```

```
      ],
      "allowedSignatureAlgorithms": [
      ],
      "authenticationType": "usernamePassword",
      "contentCollision": "reject",
      "doNotSend100Continue": false,
      "folderToMoveDataTo": "",
      "mdnSendAttemptDelaySeconds": 30,
      "mdnSendAttemptRetries": 3,
      "mdnSendAttemptTimeoutSeconds": 60,
      "micAlgorithm": "asRequestedOrSHA256",
      "myId": "AS2_1",
      "partnerCertificateFilePath": "",
      "partnerId": "AS2_2",
      "rejectIdMismatch": true,
      "rejectMessageIdCollision": true,
      "rejectNotEncrypted": true,
      "rejectNotSigned": true,
      "rejectPartnerIdMismatch": true,
      "renameFilesTo": "",
      "transactionFailedCommandSettings": {
      },
      "transactionFailedEmail": {
      },
      "transactionSuccessCommandSettings": {
      },
      "transactionSuccessEmail": {
      }
    },
    "relationships": {
    },
    "type": "AS2Inbound"
  }
}
```

PATCH PowerShell Sample

```
$update =
'{
  "data": {
    "type": "AS2Inbound",
    "attributes": {
      "myId": "AS2_1",
      "partnerId": "AS2_4",
      "partnerCertificateFilePath": "C:\\Users\\DYelacic1951\\Desktop\\certs\\ssl.crt"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
# update / patch
Write-Output "Update User specific as2inbound information"
Write-Output "-----"
$as2InboundList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/users/$userid/as2inbound"
-Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $as2InboundList | ConvertTo-Json
foreach ($user in $as2InboundList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteid}/users/{userid}/as2outbound

Returns and updates user outbound AS2 parameters

- GET
- PATCH

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/as2outbound
```

GET Body Sample

```
# @name usersList
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###

@Usersid = {{usersList.response.body.$.data[0].id}}
###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}/as2outbound HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": { "attributes": { }, "relationships": { }, "type": "AS2Outbound" } }
```

GET PowerShell Sample

```
Write-Output "Users specific as2outbound information"
Write-Output "-----"
$as2outList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/users/$userid/as2outbound"
-Method 'GET' -Headers $authHeader
```

```
Write-Output $as2outList | ConvertTo-Json
foreach ($user in $as2outList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/as2outbound
```

PATCH Body Sample

```
###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}/as2outbound HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "AS2outbound",
    "attributes": {
      "myId": "AS2_1",
      "partnerId": "AS2_4",
    "hotFolderPath": "C:\\Users\\DYelacic1951\\Desktop\\HOTBOX\\"
    }
  }
}
###
```

PATCH Response Body Sample

```
{ "data": { "attributes": { }, "relationships": { }, "type": "AS2Outbound" } }
```

PATCH PowerShell Sample

```
$update =
```

```
'{
  "data": {
    "type": "AS2outbound",
    "attributes": {
      "myId": "AS2_1",
      "partnerId": "AS2_4",
      "hotFolderPath": "C:\\Users\\DYelacic1951\\Desktop\\HOTBOX\\"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
# update / patch
Write-Output "Update User specific as2outbound information"
Write-Output "-----"
$as2outboundList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/users/$userid/as2outbound"
-Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $as2outboundList | ConvertTo-Json
foreach ($user in $as2outboundList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteid}/users/{userid}/counters

Returns user account statistics.

> **NOTE:** As of EFT 8.1, the response will include "timePasswordChanged" (see GET Response Body Sample below).

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/counters
```

GET Body Sample

```
#### GET USER DETAILS COUNTERS ####
## Must obtain User_ID##

GET https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{UserID}}/counters HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 17:43:54 GMT Content-Type:
application/vnd.api+json
Content-Length: 264 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer

{ "data": { "attributes": { "isConnected": false, "isLocked": false, "lastModifiedBy":
"admin",
"timeCreated": "2022-08-04 01:23:35 PM", "timeLastConnected": null, "timeLastModified":
"2022-08-04 01:23:35 PM", "timePasswordChanged": "2022-08-04 01:23:35 PM" }, "type":
"userCounters" } }
```

GET PowerShell Sample

```
$userid = $userList.data[0].id

# get users counters
Write-Output "Users counters"
Write-Output "-----"
$userList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users/$userid/counters"
-Method 'GET' -Headers $authHeader
Write-Output $userList | ConvertTo-Json
foreach ($user in $userList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Filesystem REST API

The endpoints described in this section are part of /sites/siteId/ related to folders.

- Endpoint: /sites/{siteId}/filesystem/folders
- Endpoint: /sites/{siteId}/filesystem/folders/{folderid}
- Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/folders
- Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/permissions
- Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/permissions/{folderpermid}

Endpoint: /sites/{siteId}/filesystem/folders

Returns folder

> **NOTE:** In v8.1 and later, includes Upload Quota Settings

- GET

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/filesystem/folders
```

GET Body Sample

```
@Siteid = {{siteList.response.body.$.data[0].id}}

###

GET https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 16:59:16 GMT Content-Type:
application/vnd.api+json ETag: "B7E6B8C3"

Content-Length: 529 Cache-Control: no-cache, no-store, must-revalidate Expires: -1

X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;

Referrer-Policy: no-referrer


 { "data": { "attributes": { "name": "", "subFolders": [ "anonymous", "Bin", "Incoming",
"Pub", "Usr" ], "target": {

 "type": "winFolder", "winFolder": { "path": "C:\\InetPub\\EFTRoot\\MySite\\" } },
"uploadQuota": null },

 "id": "%2F", "links": { "self": "/admin/v2/sites/e82de253-b8ec-4b70-a72d-
d017c3317f01/filesystem/folders/%252F" },

 "relationships": { "inheritedPermissions": { "meta": { "name": "inherited permissions"
} }, "permissions": {

 "links": { "related": "/admin/v2/sites/e82de253-b8ec-4b70-a72d-
d017c3317f01/filesystem/folders/%252F/permissions" } } },
```

```
 "type": "folder" } }
```

GET PowerShell Sample

```
$userid = $userList.data[0].id

# get users counters
Write-Output "filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/filesystem/folders"
-Method 'GET' -Headers $authHeader
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}

Returns folder settings, updates folder settings, creates folders, and deletes folders (updated on EFT 8.1, it now includes the Upload Quota Settings)

- GET
- POST
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}
```

GET Body Sample

```
##### GET the Folder structure and settings for a specifc User   #########

@User_Folder_ID = AFAR

GET https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2F{{User_Folder_ID}}%2F HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 17:04:14 GMT Content-Type: application/vnd.api+json

ETag: "95FFEAF1" Content-Length: 470 Cache-Control: no-cache, no-store, must-revalidate

Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;

Referrer-Policy: no-referrer

{ "data": { "attributes": { "name": "AFAR", "subFolders": [], "target": null, "uploadQuota": null },

"id": "%2Fusr%2FAFAR%2F", "links": { "self": "/admin/v2/sites/e82de253-b8ec-4b70-a72d-d017c3317f01/

filesystem/folders/%252Fusr%252FAFAR%252F" }, "relationships": { "inheritedPermissions": { "meta": {

"name": "inherited permissions" } }, "permissions": { "links": { "related":
```

```
"/admin/v2/sites/e82de253-b8ec-4b70-a72d-
d017c3317f01/filesystem/folders/%252Fusr%252FAFAR%252F/permissions" } } },
"type": "folder" } }
```

GET PowerShell Sample

```
# get filesystem folders
Write-Output "filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2Fusr%2F"
-Method 'GET' -Headers $authHeader
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/
{siteId}/filesystem/folders/{folderid}
```

POST Body Sample

```
###
POST https://{{host}}/admin/v2/sites/
{{Siteid}}/filesystem/folders/%2fusr%2fdyelacic%2f/folders HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
 "data": {
    "attributes": {
        "name": "HelloWorld",
        "target": {
            "type": "winFolder",
            "winFolder": {
```

```
                "path": "c:/temp"
            }
        }
    }
 }

}
```

POST Body Sample - Example II – including Upload Quotas

```
##### POST REQUEST TO CREATE A FOLDER WITH UPLOAD QUOTA ENABLED #########

@User_Folder = afar

POST https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2F{{User_
Folder}}%2F/folders HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "folder",
    "attributes": {
      "name": "Folder4",
      "subFolder": "Folder4",
    "uploadQuota": {
        "emailsToReportToOnExceed": [
          "gsqaaf1@gmail.com",
          "gsqaaf2@gmail.com"
        ],
        "enabled": true,
        "limitMBytes": 150,
        "usedMBytes": 0
      }
    }
  }
}
```

POST Response Body Sample

```
{ "data": { "attributes": { "name": "biohazard", "subFolders": [], "target": "c:/temp"
},
"id": "%2Fusr%2Fdyelacic%2Fbiohazard%2F", "links": { "self":
"/Admin/v2/sites/f1e58e70-926f-4786-877b-cf62abfdf0db/filesystem/folders/
%252Fusr%252Fdyelacic%252Fbiohazard%252F" }, "relationships": { "inheritedPermissions":
{
"meta": { "name": "inherited permissions" } }, "permissions": { "links": { "related":
"/Admin/v2/sites/f1e58e70-926f-4786-877b-cf62abfdf0db/filesystem/folders/%252Fusr%252F
dyelacic%252Fbiohazard%252F/permissions" } } }, "type": "folder" } }
```

POST PowerShell Sample

```
$update =
'{
    "data": {
        "type": "folder",
        "id": "%2Fmetallica2%2F",
        "attributes": {
            "name": "metallica2",
            "target": "c:/util"
        }
    }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 20
# update filesystem folders
Write-Output "filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2fusr%2fFranklin%2f"
-Method 'POST' -Headers $authHeader -Body $update
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/filesystem/folders/{folderid}
```

PATCH Body Sample

```
#
# change the path to where this virtual folder points
#
###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2F
test_user_sql%2Fmetallica%2F HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
      "name": "metallica",
      "subFolders": [],
      "target": {
        "type": "winFolder",
        "winFolder": {
          "path": "C:\\temp"
        }
      },
      "uploadQuota": null
    },
    "id": "%2Fusr%2Ftest_user_sql%2Fmetallica%2F",
    "type": "folder"
  }
}
###
```

PATCH Response Body Sample

```
HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 13:31:59 GMT Content-Type:
application/vnd.api+json
```

```
ETag: "B0A1B271" Content-Length: 590 Cache-Control: no-cache, no-store, must-revalidate

Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;

Referrer-Policy: no-referrer { "data": { "attributes": { "name": "metallica",
"subFolders": [],

"target": { "type": "winFolder", "winFolder": { "path": "C:\\temp" } }, "uploadQuota":
null },

"id": "%2Fusr%2Ftest_user_sql%2Fmetallica%2F", "links": { "self":

"/admin/v2/sites/7c2d15e3-e151-4029-8aa2-d4475296ba1c/filesystem/folders/%252Fusr%252F

test_user_sql%252Fmetallica%252F" }, "relationships": { "inheritedPermissions": {
"meta": {

"name": "inherited permissions" } }, "permissions": { "links": { "related":
"/admin/v2/sites/

7c2d15e3-e151-4029-8aa2-d4475296ba1c/filesystem/folders/%252Fusr%252Ftest_user_
sql%252Fmetallica%252F

/permissions" } } }, "type": "folder" } }
```

PATCH PowerShell Sample

```
#

# renaming the virtual folder name

#

$update =

'{

  "data": {

    "attributes": {

      "name": "metallica",

      "subFolders": [],

      "target": {

        "type": "winFolder",

        "winFolder": {

          "path": "C:\\temp"

        }

      },

      "uploadQuota": null

    },

    "id": "%2Fusr%2Ftest_user_sql%2Fmetallica%2F",

    "type": "folder"

  }
```

```
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 20
# update filesystem folders
Write-Output "patch filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2fusr%2fdyelacic%2fmetallica%2f"
-Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/
{siteId}/filesystem/folders/{folderid}
```

DELETE Body Sample

```
###
DELETE https://{{host}}/admin/v2/sites/
{{Siteid}}/filesystem/folders/%2Fusr%2FFranklin%2F HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Thu, 10 Feb 2022 14:49:46 GMT Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
Write-Output "delete filesystem folders"

Write-Output "-----"

$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2Fusr%2Fdyelacic%2F"

-Method 'DELETE' -Headers $authHeader

Write-Output $folderList | ConvertTo-Json

foreach ($user in $folderList.data)

{

    Write-Output ("User $($user.id): $($user.attributes.loginName)")

}
```

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/folders

Creates physical or virtual sub-folder

- POST

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/
{siteId}/filesystem/folders/{folderid}/folders
```

POST Body Sample

```
#
# creating a physical sub folder below the users home folder
#
###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2Fdyelacic%2F/
folders HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "type": "folder",
    "attributes": {
      "name": "tuneroom",
      "subFolder": "tuneroom"
    }
  }
}
###
```

POST Response Body Sample

```
{ "data": { "attributes": { "name": "tuneroom", "subFolders": [], "target": null },
"id":
```

```
"%2Fusr%2Fdyelacic%2Ftuneroom%2F", "links": { "self": "/Admin/v2/sites/f1e58e70-926f-
4786-877b-cf62abfdf0db/

filesystem/folders/%252Fusr%252Fdyelacic%252Ftuneroom%252F" }, "relationships": {
"inheritedPermissions": {

"meta": { "name": "inherited permissions" } }, "permissions": { "links": { "related":

"/Admin/v2/sites/f1e58e70-926f-4786-877b-
cf62abfdf0db/filesystem/folders/%252Fusr%252Fdyelacic%25

2Ftuneroom%252F/permissions" } } }, "type": "folder" } }
```


POST PowerShell Sample

```
#

# create physical sub folder below users home folder

#

$update =

'{

    "data": {

        "type": "folder",

        "attributes": {

            "name": "sunroom",

            "subFolder": "sunroom"

        }

    }

}'

$update = $update | ConvertFrom-Json

$update = $update | ConvertTo-Json -Depth 20

# create filesystem folders

Write-Output "create sub folder"

Write-Output "-----"

$folderList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/filesystem/

folders/%2fusr%2fdyelacic%2f/folders"

-Method 'POST' -Headers $authHeader -Body $update

Write-Output $folderList | ConvertTo-Json

foreach ($user in $folderList.data)

{

    Write-Output ("User $($user.id): $($user.attributes.loginName)")

}
```

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/permissions

Returns a list of permissions for a specific folder, adding existing permissions to a specific folder.

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/filesystem/folders/{folderid}/permissions
```

GET Body Sample

```
# get folder permissions

#

###

GET https://{{host}}/admin/v2/sites/
{{Siteid}}/filesystem/folders/%2Fusr%2Fdyelacic%2F/permissions HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample

```
{ "data": [ { "attributes": { "canAppendFile": true, "canCreateSubfolder": true,

"canDeleteFile": true, "canDeleteSubfolder": true, "canDownloadFile": true, "canList":

true, "canRenameFileOrSubfolder": true, "canSeeHiddenFileOrSubfolder": true,
"canSeeInParentList":

true, "canSeeReadOnlyFileOrSubfolder": true, "canUploadFile": true }, "links": { "self":
"/Admin/v2/sites/

f1e58e70-926f-4786-877b-cf62abfdf0db/filesystem/folders/%252Fusr%252Fdyelacic%252F/

permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281" }, "relationships": { "trustee":
{ "data": {

"id": "04dcfd20-fc73-41d0-a0d8-62d1706e6281", "meta": { "name": "dyelacic" }, "type":
"user" },

"links": { "related": "/Admin/v2/sites/f1e58e70-926f-4786-877b-cf62abfdf0db/users/

04dcfd20-fc73-41d0-a0d8-62d1706e6281" } } }, "type": "folderPermissions" } ] }
```

GET PowerShell Sample

```
#
# get filesystem folders permissions
Write-Output "filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/filesystem/folders/
%2Fusr%2Fdyelacic%2f/permissions" -Method 'GET' -Headers $authHeader
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/
{siteId}/filesystem/folders/{folderid}/permissions
```

POST Body Sample

```
###
#Add / Link folder to an existing user permissions group.

POST https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/
%2Fusr%2Ftest_user_sql%2Fspam%2F/permissions HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data":
    {
      "type": "folderPermissions",
      "attributes": {
        "canAppendFile": true,
        "canCreateSubfolder": true,
        "canDeleteFile": true,
        "canDeleteSubfolder": true,
        "canDownloadFile": true,
```

```
        "canList": true,
        "canRenameFileOrSubfolder": true,
        "canSeeHiddenFileOrSubfolder": true,
        "canSeeInParentList": true,
        "canSeeReadOnlyFileOrSubfolder": true,
        "canUploadFile": false
      },
      "relationships": {
        "trustee": {
          "data": {
            "type": "userGroup",
            "id": " b8448b77-01d8-47d5-8ee7-9f407c95e39f",
            "meta": {
              "name": "Guests"
            }
          }
        }
      }
    }
 }
###
```

POST Response Body Sample

```
HTTP/1.1 201 Created Date: Thu, 18 Aug 2022 19:32:43 GMT Location: /admin/v2/sites/
7c2d15e3-e151-4029-8aa2-d4475296ba1c/filesystem/folders/%252Fusr%252Ftest_user_
sql%252Fspam%252F/
permissions/group-b8448b77-01d8-47d5-8ee7-9f407c95e39f Content-Type:
application/vnd.api+json
ETag: "C5020903" Content-Length: 774 Cache-Control: no-cache, no-store, must-revalidate
Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer { "data": { "attributes": { "canAppendFile": true,
"canCreateSubfolder": true, "canDeleteFile": true, "canDeleteSubfolder": true,
"canDownloadFile": true, "canList": true, "canRenameFileOrSubfolder": true,
"canSeeHiddenFileOrSubfolder": true, "canSeeInParentList": true,
"canSeeReadOnlyFileOrSubfolder": true, "canUploadFile": false }, "links": { "self":
"/admin/v2/sites/7c2d15e3-e151-4029-8aa2-d4475296ba1c/filesystem/folders/%252Fusr%252F
```

```
test_user_sql%252Fspam%252F/permissions/group-b8448b77-01d8-47d5-8ee7-9f407c95e39f" },
"relationships": { "trustee": { "data": { "type": "userGroup", "id": "b8448b77-01d8-
47d5-8ee7-9f407c95e39f",
"meta": { "name": "Guests" } }, "links": { "related": "/admin/v2/sites/7c2d15e3-e151-
4029-8aa2-d4475296ba1c/
user-groups/b8448b77-01d8-47d5-8ee7-9f407c95e39f" } } }, "type": "folderPermissions" } }
```

POST PowerShell Sample

```
#
# Add an existing user permissions group to a folder
$update =
'{
  "data":
    {
      "type": "folderPermissions",
      "attributes": {
        "canAppendFile": true,
        "canCreateSub    folder": true,
        "canDeleteFile": true,
        "canDeleteSubfolder": true,
        "canDownloadFile": true,
        "canList": true,
        "canRenameFileOrSubfolder": true,
        "canSeeHiddenFileOrSubfolder": true,
        "canSeeInParentList": true,
        "canSeeReadOnlyFileOrSubfolder": true,
        "canUploadFile": false
      },
      "relationships": {
        "trustee": {
          "data": {
            "type": "userGroup",
            "id": "b8448b77-01d8-47d5-8ee7-9f407c95e39f",
            "meta": {
              "name": "Guests"
            }
          }
```

```
        }
      }
    }
 }’
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
# add sub folder permissions
Write-Output "add sub folder permissions"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/filesystem/folders/
%2fusr%2fdyelacic%2ftuneroom%2f/permissions" -Method 'POST' -Headers $authHeader -Body
$update
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/permissions/{folderpermid}

Returns, updates, and deletes permissions on folder

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/
{siteId}/filesystem/folders/{folderid}/permissions/
{folderpermid}
```

GET Body Sample

```
# get the permissions for a specific folder

#

###

GET https://{{host}}/admin/v2/sites/
{{Siteid}}/filesystem/folders/%2Fusr%2Fdyelacic%2Fsunroom%2F/

permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281 HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample

```
{ "data": { "attributes": { "canAppendFile": true, "canCreateSubfolder": true,
"canDeleteFile": true,

"canDeleteSubfolder": true, "canDownloadFile": false, "canList": true,
"canRenameFileOrSubfolder": true,

"canSeeHiddenFileOrSubfolder": true, "canSeeInParentList": true,
"canSeeReadOnlyFileOrSubfolder": true,

"canUploadFile": true }, "links": { "self": "/Admin/v2/sites/f1e58e70-926f-4786-877b-
cf62abfdf0db/

filesystem/folders/%252Fusr%252Fdyelacic%252Fsunroom%252F/permissions

/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281" }, "relationships": { "trustee": { "data": {
```

```
"id": "04dcfd20-fc73-41d0-a0d8-62d1706e6281", "meta": { "name": "dyelacic" }, "type":
"user" },
"links": { "related": "/Admin/v2/sites/f1e58e70-926f-4786-877b-cf62abfdf0db/users/
04dcfd20-fc73-41d0-a0d8-62d1706e6281" } } }, "type": "folderPermissions" } }
```

GET PowerShell Sample

```
# get the folders permission
# get filesystem folders permissions
Write-Output "filesystem folders permissions"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2Fusr%2Fdyelacic%2fsunroom%2f/
permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281" -Method 'GET' -Headers
$authHeader
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/
{siteId}/filesystem/folders/{folderid}/permissions/
{folderpermid}
```

PATCH Body Sample

```
# change / update folder permissions
###
PATCH https://{{host}}/admin/v2/sites/
{{Siteid}}/filesystem/folders/%2Fusr%2Fdyelacic%2Fsunroom%2F/
permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281 HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "type": "folderPermissions",
```

```
    "attributes": {
      "canUploadFile": false,
      "canDownloadFile": true,
      "canDeleteFile": false,
      "canRenameFileOrSubfolder": true,
      "canAppendFile": true,
      "canDeleteSubfolder": false,
      "canCreateSubfolder": true,
      "canSeeHiddenFileOrSubfolder": true,
      "canSeeReadOnlyFileOrSubfolder": true,
      "canSeeInParentList": true,
      "canList": true
    }
  }
}
###
```

PATCH Response Body Sample

```
{ "data": { "attributes": { "canAppendFile": true, "canCreateSubfolder": true,
"canDeleteFile":
false, "canDeleteSubfolder": false, "canDownloadFile": true, "canList": true,
"canRenameFileOrSubfolder": true, "canSeeHiddenFileOrSubfolder": true,
"canSeeInParentList": true,
"canSeeReadOnlyFileOrSubfolder": true, "canUploadFile": false }, "links": { "self":
"/Admin/v2/sites/f1e58e70-926f-4786-877b-cf62abfdf0db/filesystem/folders/%252Fusr%252F
dyelacic%252Fsunroom%252F/permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281" },
"relationships": { "trustee": { "data": { "id": "04dcfd20-fc73-41d0-a0d8-62d1706e6281",
"meta": { "name": "dyelacic" }, "type": "user" }, "links": { "related":
"/Admin/v2/sites/f1e58e70-926f-4786-877b-cf62abfdf0db/users/04dcfd20-fc73-41d0-a0d8-
62d1706e6281" } } },
"type": "folderPermissions" } }
```

PATCH PowerShell Sample

```
# change folder permissions
$update =
```

```
'{
  "data": {
    "type": "folderPermissions",
    "attributes": {
      "canUploadFile": false,
      "canDownloadFile": true,
      "canDeleteFile": false,
      "canRenameFileOrSubfolder": true,
      "canAppendFile": true,
      "canDeleteSubfolder": false,
      "canCreateSubfolder": true,
      "canSeeHiddenFileOrSubfolder": true,
      "canSeeReadOnlyFileOrSubfolder": true,
      "canSeeInParentList": true,
      "canList": true
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
# change folder permissions
Write-Output "change folder permissions"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/
filesystem/folders/%2fusr%2fdyelacic%2ftuneroom%2f/permissions/
user-04dcfd20-fc73-41d0-a0d8-62d1706e6281" -Method 'PATCH'
-Headers $authHeader -Body $update
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/
{siteId}/filesystem/folders/{folderid}/permissions/
{folderpermid}
```

DELETE Body Sample

```
# delete folder permissions


###

DELETE https://{{host}}/admin/v2/sites/
{{Siteid}}/filesystem/folders/%2Fusr%2Fdyelacic%2Fsunroom%2F/permissions/user-04dcfd20-
fc73-41d0-a0d8-62d1706e6281 HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Fri, 11 Feb 2022 22:06:08 GMT Content-Length: 0

Cache-Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options:
nosniff

X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self' 'unsafe-
inline'

'unsafe-eval' data:; Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
#

# delete folder permissions


Write-Output "delete folders permissions"

Write-Output "-----"

$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2Fusr

%2Fdyelacic%2ftuneroom%2f/permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281"

-Method 'DELETE' -Headers $authHeader

Write-Output $folderList | ConvertTo-Json

foreach ($user in $folderList.data)

{

    Write-Output ("User $($user.id): $($user.attributes.loginName)")

}
```

Event Rules REST API

The endpoints described in this section are part of /sites/siteId/ related to event rules.

- Endpoint: /sites/{siteid}/event-rules
- Endpoint: /sites/{siteid}/event-rules/{ruleid}
- Endpoint: /sites/{siteid}/event-rule-folders/{folderid}
- Endpoint: /sites/{siteid}/event-rule-folders

Endpoint: /sites/{siteid}/event-rules

Get or create site event rules

- GET
- POST

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rules
```

GET Body Sample

```
### GET SITE EVENT RULES ###

GET https://{{host}}/admin/v2/sites/{{Siteid}}/event-rules HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###
```

GET Response Body Sample


```
{"data":[{"type":"eventRule","id":"8d11ec4f-3c6c-4ab9-8045-fb5c94b38ca0","attributes":
{"info":{

"Description":"Backup and Cleanup","Enabled":true,"Folder":"00000000-0000-0000-0000-
000000000000",

"Name":"Backup and Cleanup","Next":"a220530d-c190-4fa8-ae4a-
52240f6fee94","Remote":false,"Type":"Timer",

"apiVersion":"v2","eventRuleVersion":"416"},"statements":{"StatementsList":
[{"ActionStatement":{"Action":{

"CleanupAction":{"DaysToKeepFiles":30,"FileMask":"*.bak","Folder":

"C:\\ProgramData\\Globalscape\\EFT
Server\\Backup","Include":true,"Recursive":false,"TimestampType":"Both"}},

"IfFailedActions":[]},"ConditionStatement":{"Conditions":[],"ElseAttachedStatements":[],

"IfAttachedStatements":[],"Operator":"Or"},"LoopDatasetStatement":{"Params":
{"DatasetName":"",

"EndLoopRow":0,"OrderingColumn":"","SortOrder":"Original","StartLoopRow":0,"UseEndLoopRo
w":false,

"UseStartLoopRow":false},"Statements":[]},"Type":"Action"},{"ActionStatement":{"Action":
{"CleanupAction":{

"DaysToKeepFiles":30,"FileMask":"*.*","Folder":"C:\\ProgramData\\Globalscape\\EFT
Server\\Logs",
```

```
"Include":true,"Recursive":false,"TimestampType":"Both"}},"IfFailedActions":
[]},"ConditionStatement":{

"Conditions":[],"ElseAttachedStatements":[],"IfAttachedStatements":[],"Operator":"Or"},

"LoopDatasetStatement":{"Params":
{"DatasetName":"","EndLoopRow":0,"OrderingColumn":"","SortOrder":

"Original","StartLoopRow":0,"UseEndLoopRow":false,"UseStartLoopRow":false},"Statements":
[]},

"Type":"Action"},{"ActionStatement":{"Action":{"BackupServerAction":{"Path":

"C:\\ProgramData\\Globalscape\\EFT Server\\Backup"}},"IfFailedActions":[{"StopAction":{

"Enabled":false,"Result":"StopThisRule"}}]},"ConditionStatement":{"Conditions":
[],"ElseAttachedStatements":[],

"IfAttachedStatements":[],"Operator":"Or"},"LoopDatasetStatement":{"Params":
{"DatasetName":"",

"EndLoopRow":0,"OrderingColumn":"","SortOrder":"Original","StartLoopRow":0,"UseEndLoopRo
w":false,

"UseStartLoopRow":false},"Statements":[]},"Type":"Action"}]},"trigger":{"TimerParams":
{"DailyInfo":{

"DayPeriod":1,"EveryWeekDay":true},"EndDateEnabled":false,"EndDateTime":1659675600,"EndT
imeEnabled":false,

"HolidayCalendarID":"00000000-0000-0000-0000-000000000000","MonthlyInfo":
{"DayPeriod":1,"MonthPeriod":1,

"RelativeDay":"First","UseFixedDayIndexInMonth":true,"Weekday":"Sunday"},"Recurrence":"D
aily",

"RepeatEnabled":false,"RepeatPattern":"Hours","RepeatRate":1,"RundayCalendarID":

"00000000-0000-0000-0000-000000000000","StartDateTime":1659675600,"WeeklyInfo":
{"WeekDayFlags":1,

"WeekPeriod":1},"YearlyInfo":{"DayPeriod":1,"Month":"January","RelativeDay":"First",

"UseFixedDayIndexInFixedMonth":true,"Weekday":"Sunday"}}},"link":{"self":

"/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/event-rules/8d11ec4f-3c6c-4ab9-
8045-fb5c94b38ca0"}},

{"type":"eventRule","id":"a220530d-c190-4fa8-ae4a-52240f6fee94","attributes":{"info":
{"Description":

"Execute a specified action one time or repeat at a specified
interval.","Enabled":true,"Folder":

"00000000-0000-0000-0000-000000000000","Name":"SendToDrobinson","Next":"00000000-0000-
0000-0000-000000000000",

"Remote":false,"Type":"Timer","apiVersion":"v2","eventRuleVersion":"416"},"statements":{

"StatementsList":[{"ActionStatement":{"Action":null,"IfFailedActions":
[]},"ConditionStatement":{

"Conditions":
[{"ContextVariable":"","Negate":false,"Operator":"Equals","PropertyID":1000,"Value":{

"Flag":false,"Value":"Yes"}}],"ElseAttachedStatements":[],"IfAttachedStatements":
[{"ActionStatement":{

"Action":{"UploadAction":{"ConnectionProfileGUID":"00000000-0000-0000-0000-
000000000000","LocalPath":
```

```
"C:\\Users\\Administrator\\Desktop\\EFT.exe","RemotePath":"/%SOURCE.FILE_
NAME%","RemoveSource":false,

"TransferSettings":{"Connection":{"CertificateSettings":{"CertId":"00000000-0000-0000-
0000-000000000000",

"CertPath":"","KeyPath":"","Passphrase":"UpKUJq1sD4Yfb1Hz8ZFiRw=="},"EnableAutoLogin":fa
lse,

"Host":"10.91.160.102","Password":"t7aoT+M7wIt7hzqlvPd+7g==","Port":"22","Protocol":"SFT
P",

"TrustedPubKey":"","User":"drobinson"},"Transfer":{"ASCIIFileExts":
["TXT","INF","HTML","HTM"],

"ClearCommandChannel":false,"ClearDataChannel":false,"ConnectionTimeout":30,"CustomProxy
Commands":[],

"DataPortMode":"AUTO","DelayBetweenRetries":30,"HomeIP":"0.0.0.0","HostName":"","MaxConc
urrentThreads":1,

"NumberOfConnectionRetries":0,"PASVPortMax":65535,"PASVPortMin":0,"Password":

"UpKUJq1sD4Yfb1Hz8ZFiRw==","Port":21,"PreserveLocalTimeStamp":false,"PreserveRemoteTimeS
tamp":false,

"ProxySeparator":"@","ProxySubType":0,"ProxyType":"FTP","SOCKSSettings":
{"Auth":false,"HostName":"",

"Password":"UpKUJq1sD4Yfb1Hz8ZFiRw==","Port":1080,"Type":"None","Use":false,"UserNam
e":""},

"TransferEncoding":"UTF8","UseProxy":false,"UserName":"","ValidateFileIntegrity":false},

"TransferAdditional":
{"DeleteSourceIfMoveSkipped":true,"OverwriteType":"Overwrite","PrePostCommandSettings":{

"ContinueOnFailPost":false,"ContinueOnFailPre":false,"PostCommandArg":"","PostCommandArg
Delimiter":32,

"PostCommandType":"None","PreCommandArg":"","PreCommandType":"None"},"RenameDestinationF
ile":false,

"RenameDestinationFileTo":"","SyncSettings":
{"SyncDeleteFileIfNotPresent":false,"SyncDirectionType":"MirrorRemote",

"SyncFolders":false,"SyncIncludeSubfolders":false,"SyncOverwriteType":"Overwrite"},

"TreatMissingSourceAsSuccess":false}}}},"IfFailedActions":[{"StopAction":
{"Enabled":false,

"Result":"StopThisRule"}}]},"ConditionStatement":{"Conditions":
[],"ElseAttachedStatements":[],

"IfAttachedStatements":[],"Operator":"Or"},"LoopDatasetStatement":{"Params":
{"DatasetName":"",

"EndLoopRow":0,"OrderingColumn":"","SortOrder":"Original","StartLoopRow":0,"UseEndLoopRo
w":false,

"UseStartLoopRow":false},"Statements":
[]},"Type":"Action"}],"Operator":"And"},"LoopDatasetStatement":{

"Params":
{"DatasetName":"","EndLoopRow":0,"OrderingColumn":"","SortOrder":"Original","StartLoopRo
w":0,

"UseEndLoopRow":false,"UseStartLoopRow":false},"Statements":
[]},"Type":"Condition"}]},"trigger":{
```

```
"TimerParams":{"DailyInfo":{"DayPeriod":1,"EveryWeekDay":true},"EndDateEnabled":false,
"EndDateTime":1659710856,"EndTimeEnabled":false,"HolidayCalendarID":"00000000-0000-0000-
0000-000000000000",
"MonthlyInfo":
{"DayPeriod":1,"MonthPeriod":1,"RelativeDay":"First","UseFixedDayIndexInMonth":true,
"Weekday":"Sunday"},"Recurrence":"Continually","RepeatEnabled":true,"RepeatPattern":"Min
utes",
"RepeatRate":8,"RundayCalendarID":"00000000-0000-0000-0000-
000000000000","StartDateTime":1659710856,
"WeeklyInfo":{"WeekDayFlags":1,"WeekPeriod":1},"YearlyInfo":
{"DayPeriod":1,"Month":"January",
"RelativeDay":"First","UseFixedDayIndexInFixedMonth":true,"Weekday":"Sunday"}}}},"link":
{"self":
"/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/event-rules/a220530d-c190-4fa8-
ae4a-52240f6fee94"}}]}
```


GET PowerShell Sample

```
### Returns event rule settings ###
### User must obtain the SiteID from Get Sites
Write-Output "ER"
Write-Output "----"
#$siteID = Enter SiteID here
$ERList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rules"
-Method 'GET' -Headers $authHeader
Write-Output $ERList | ConvertTo-Json
```

Method & URL

```
POST https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rules
```

POST Body Sample

```
### CREATE EVENT RULES ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/event-rules HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
```

```
      "type": "eventRule",
      "id": "a220530d-c190-4fa8-ae4a-52240f6fee94",
      "attributes": {
        "info": {
          "Description": "Execute a specified action one time or repeat at a specified
interval.",
          "Enabled": true,
          "Folder": "00000000-0000-0000-0000-000000000000",
          "Name": "SendToDrobinson",
          "Next": "00000000-0000-0000-0000-000000000000",
          "Remote": false,
          "Type": "Timer",
          "apiVersion": "v2",
          "eventRuleVersion": "416"
        },
        "statements": {
          "StatementsList": [
            {
              "ActionStatement": {
                "Action": null,
                "IfFailedActions": []
              },
              "ConditionStatement": {
                "Conditions": [
                  {
                    "ContextVariable": "",
                    "Negate": false,
                    "Operator": "Equals",
                    "PropertyID": 1000,
                    "Value": {
                      "Flag": false,
                      "Value": "Yes"
                    }
                  }
                ],
                "ElseAttachedStatements": [],
                "IfAttachedStatements": [
                  {
```

```
                    "ActionStatement": {
                      "Action": {
                        "UploadAction": {
                          "ConnectionProfileGUID": "00000000-0000-0000-0000-
000000000000",
                          "LocalPath": "C:\\Users\\Administrator\\Desktop\\EFT.exe",
                          "RemotePath": "/%SOURCE.FILE_NAME%",
                          "RemoveSource": false,
                          "TransferSettings": {
                            "Connection": {
                              "CertificateSettings": {
                                "CertId": "00000000-0000-0000-0000-000000000000",
                                "CertPath": "",
                                "KeyPath": "",
                                "Passphrase": "UpKUJq1sD4Yfb1Hz8ZFiRw=="
                              },
                              "EnableAutoLogin": false,
                              "Host": "10.91.160.102",
                              "Password": "t7aoT+M7wIt7hzqlvPd+7g==",
                              "Port": "22",
                              "Protocol": "SFTP",
                              "TrustedPubKey": "",
                              "User": "drobinson"
                            },
                            "Transfer": {
                              "ASCIIFileExts": [
                                "TXT",
                                "INF",
                                "HTML",
                                "HTM"
                              ],
                              "ClearCommandChannel": false,
                              "ClearDataChannel": false,
                              "ConnectionTimeout": 30,
                              "CustomProxyCommands": [],
                              "DataPortMode": "AUTO",
                              "DelayBetweenRetries": 30,
                              "HomeIP": "0.0.0.0",
```

```
    "HostName": "",
    "MaxConcurrentThreads": 1,
    "NumberOfConnectionRetries": 0,
    "PASVPortMax": 65535,
    "PASVPortMin": 0,
    "Password": "UpKUJq1sD4Yfb1Hz8ZFiRw==",
    "Port": 21,
    "PreserveLocalTimeStamp": false,
    "PreserveRemoteTimeStamp": false,
    "ProxySeparator": "@",
    "ProxySubType": 0,
    "ProxyType": "FTP",
    "SOCKSSettings": {
      "Auth": false,
      "HostName": "",
      "Password": "UpKUJq1sD4Yfb1Hz8ZFiRw==",
      "Port": 1080,
      "Type": "None",
      "Use": false,
      "UserName": ""
    },
    "TransferEncoding": "UTF8",
    "UseProxy": false,
    "UserName": "",
    "ValidateFileIntegrity": false
  },
  "TransferAdditional": {
    "DeleteSourceIfMoveSkipped": true,
    "OverwriteType": "Overwrite",
    "PrePostCommandSettings": {
      "ContinueOnFailPost": false,
      "ContinueOnFailPre": false,
      "PostCommandArg": "",
      "PostCommandArgDelimiter": 32,
      "PostCommandType": "None",
      "PreCommandArg": "",
      "PreCommandType": "None"
```

```
            },
            "RenameDestinationFile": false,
            "RenameDestinationFileTo": "",
            "SyncSettings": {
              "SyncDeleteFileIfNotPresent": false,
              "SyncDirectionType": "MirrorRemote",
              "SyncFolders": false,
              "SyncIncludeSubfolders": false,
              "SyncOverwriteType": "Overwrite"
            },
            "TreatMissingSourceAsSuccess": false
          }
        }
      }
    },
    "IfFailedActions": [
      {
        "StopAction": {
          "Enabled": false,
          "Result": "StopThisRule"
        }
      }
    ]
  },
  "ConditionStatement": {
    "Conditions": [],
    "ElseAttachedStatements": [],
    "IfAttachedStatements": [],
    "Operator": "Or"
  },
  "LoopDatasetStatement": {
    "Params": {
      "DatasetName": "",
      "EndLoopRow": 0,
      "OrderingColumn": "",
      "SortOrder": "Original",
      "StartLoopRow": 0,
```

```
                    "UseEndLoopRow": false,
                    "UseStartLoopRow": false
                  },
                  "Statements": []
                },
                "Type": "Action"
              }
            ],
            "Operator": "And"
          },
          "LoopDatasetStatement": {
            "Params": {
              "DatasetName": "",
              "EndLoopRow": 0,
              "OrderingColumn": "",
              "SortOrder": "Original",
              "StartLoopRow": 0,
              "UseEndLoopRow": false,
              "UseStartLoopRow": false
            },
            "Statements": []
          },
          "Type": "Condition"
        }
      ]
    },
    "trigger": {
      "TimerParams": {
        "DailyInfo": {
          "DayPeriod": 1,
          "EveryWeekDay": true
        },
        "EndDateEnabled": false,
        "EndDateTime": 1659710856,
        "EndTimeEnabled": false,
        "HolidayCalendarID": "00000000-0000-0000-0000-000000000000",
        "MonthlyInfo": {
```

```
              "DayPeriod": 1,
              "MonthPeriod": 1,
              "RelativeDay": "First",
              "UseFixedDayIndexInMonth": true,
              "Weekday": "Sunday"
            },
            "Recurrence": "Continually",
            "RepeatEnabled": true,
            "RepeatPattern": "Minutes",
            "RepeatRate": 8,
            "RundayCalendarID": "00000000-0000-0000-0000-000000000000",
            "StartDateTime": 1659710856,
            "WeeklyInfo": {
              "WeekDayFlags": 1,
              "WeekPeriod": 1
            },
            "YearlyInfo": {
              "DayPeriod": 1,
              "Month": "January",
              "RelativeDay": "First",
              "UseFixedDayIndexInFixedMonth": true,
              "Weekday": "Sunday"
            }
          }
        }
    }
  }
}
###
```

POST Response Body Sample

```
{"data":{"data":[{"type":"eventRule","id":"c2320fbb-e7cc-4fde-8b41-
ffa655e71e50","attributes":{"info":{

"Description":"Execute a specified action one time or repeat at a specified
interval.","Enabled":true,

"Folder":"00000000-0000-0000-0000-000000000000","Name":"SendToDrobinson",
```

```
"Next":"00000000-0000-0000-0000-
000000000000","Remote":false,"Type":"Timer","apiVersion":"v2",

"eventRuleVersion":"416"},"statements":{"StatementsList":[{"ActionStatement":
{"Action":null,

"IfFailedActions":[]},"ConditionStatement":{"Conditions":
[{"ContextVariable":"","Negate":false,

"Operator":"Equals","PropertyID":1000,"Value":
{"Flag":false,"Value":"Yes"}}],"ElseAttachedStatements":[],

"IfAttachedStatements":[{"ActionStatement":{"Action":{"UploadAction":{

"ConnectionProfileGUID":"00000000-0000-0000-0000-000000000000","LocalPath":

"C:\\Users\\Administrator\\Desktop\\EFT.exe","RemotePath":"/%SOURCE.FILE_NAME%",

"RemoveSource":false,"TransferSettings":{"Connection":{"CertificateSettings":{

"CertId":"00000000-0000-0000-0000-
000000000000","CertPath":"","KeyPath":"","Passphrase":"UpKUJq1sD4Yfb1Hz8ZFiRw=="},

"EnableAutoLogin":false,"Host":"10.91.160.102","Password":"t7aoT+M7wIt7hzqlvPd+7g==","Po
rt":"22","Protocol":"SFTP",

"TrustedPubKey":"","User":"drobinson"},"Transfer":{"ASCIIFileExts":
["TXT","INF","HTML","HTM"],

"ClearCommandChannel":false,"ClearDataChannel":false,"ConnectionTimeout":30,"CustomProxy
Commands":[],

"DataPortMode":"AUTO","DelayBetweenRetries":30,"HomeIP":"0.0.0.0","HostName":"","MaxConc
urrentThreads":1,

"NumberOfConnectionRetries":0,"PASVPortMax":65535,"PASVPortMin":0,"Password":"UpKUJq1sD4
Yfb1Hz8ZFiRw==",

"Port":21,"PreserveLocalTimeStamp":false,"PreserveRemoteTimeStamp":false,"ProxySeparato
r":"@",

"ProxySubType":0,"ProxyType":"FTP","SOCKSSettings":
{"Auth":false,"HostName":"","Password":"UpKUJq1sD4Yfb1Hz8ZFiRw==",

"Port":1080,"Type":"None","Use":false,"UserName":""},"TransferEncoding":"UTF8","UseProxy
":false,"UserName":"",

"ValidateFileIntegrity":false},"TransferAdditional":
{"DeleteSourceIfMoveSkipped":true,"OverwriteType":"Overwrite",

"PrePostCommandSettings":
{"ContinueOnFailPost":false,"ContinueOnFailPre":false,"PostCommandArg":"",

"PostCommandArgDelimiter":32,"PostCommandType":"None","PreCommandArg":"","PreCommandType
":"None"},

"RenameDestinationFile":false,"RenameDestinationFileTo":"","SyncSettings":
{"SyncDeleteFileIfNotPresent":false,

"SyncDirectionType":"MirrorRemote","SyncFolders":false,"SyncIncludeSubfolders":false,"Sy
ncOverwriteType":

"Overwrite"},"TreatMissingSourceAsSuccess":false}}}},"IfFailedActions":[{"StopAction":
{"Enabled":false,

"Result":"StopThisRule"}}]},"ConditionStatement":{"Conditions":
[],"ElseAttachedStatements":[],"IfAttachedStatements":[],

"Operator":"Or"},"LoopDatasetStatement":{"Params":
{"DatasetName":"","EndLoopRow":0,"OrderingColumn":"",
```

```
"SortOrder":"Original","StartLoopRow":0,"UseEndLoopRow":false,"UseStartLoopRow":false},"
Statements":[]},"Type":"Action"}],

"Operator":"And"},"LoopDatasetStatement":{"Params":
{"DatasetName":"","EndLoopRow":0,"OrderingColumn":"",

"SortOrder":"Original","StartLoopRow":0,"UseEndLoopRow":false,"UseStartLoopRow":false},"
Statements":[]},"Type":

"Condition"}]},"trigger":{"TimerParams":{"DailyInfo":
{"DayPeriod":1,"EveryWeekDay":true},"EndDateEnabled":false,

"EndDateTime":1659710856,"EndTimeEnabled":false,"HolidayCalendarID":"00000000-0000-0000-
0000-000000000000",

"MonthlyInfo":
{"DayPeriod":1,"MonthPeriod":1,"RelativeDay":"First","UseFixedDayIndexInMonth":true,"Wee
kday":"Sunday"},

"Recurrence":"Continually","RepeatEnabled":true,"RepeatPattern":"Minutes","RepeatRate":
8,

"RundayCalendarID":"00000000-0000-0000-0000-
000000000000","StartDateTime":1659710856,"WeeklyInfo":{"WeekDayFlags":1,

"WeekPeriod":1},"YearlyInfo":
{"DayPeriod":1,"Month":"January","RelativeDay":"First","UseFixedDayIndexInFixedMonth":tr
ue,

"Weekday":"Sunday"}}}},"link":{"self":"/admin/v2/sites/6203305a-d7c6-499e-a59b-
81500765f8f2/

event-rules/c2320fbb-e7cc-4fde-8b41-ffa655e71e50"}}]},"links":{"self":"/admin/v2/sites/

6203305a-d7c6-499e-a59b-81500765f8f2/event-rules-all/"}}
```


POST PowerShell Sample

```
### CREATE EVENT RULES ###

##POST SITE EVENT RULE settings

Write-Output "Site Event POST"

Write-Output "-----"

$update =


'{
  "data": {
      "type": "eventRule",
      "attributes": {
        "info": {
          "Description": "Execute a specified action one time or repeat at a specified
interval.",
          "Enabled": true,
          "Folder": "00000000-0000-0000-0000-000000000000",
          "Name": "SecondSendToDrobinson",
```

```
          "Next": "00000000-0000-0000-0000-000000000000",
          "Remote": false,
          "Type": "Timer",
          "apiVersion": "v2",
          "eventRuleVersion": "416"
        },
        "statements": {
          "StatementsList": [
            {
              "ActionStatement": {
                "Action": null,
                "IfFailedActions": []
              },
              "ConditionStatement": {
                "Conditions": [
                  {
                    "ContextVariable": "",
                    "Negate": false,
                    "Operator": "Equals",
                    "PropertyID": 1000,
                    "Value": {
                      "Flag": false,
                      "Value": "Yes"
                    }
                  }
                ],
                "ElseAttachedStatements": [],
                "IfAttachedStatements": [
                  {
                    "ActionStatement": {
                      "Action": {
                        "UploadAction": {
                          "ConnectionProfileGUID": "00000000-0000-0000-0000-
000000000000",
                          "LocalPath": "C:\\Users\\Administrator\\Desktop\\EFT.exe",
                          "RemotePath": "/%SOURCE.FILE_NAME%",
                          "RemoveSource": false,
                          "TransferSettings": {
```

```
                    "Connection": {
                      "CertificateSettings": {
                        "CertId": "00000000-0000-0000-0000-000000000000",
                        "CertPath": "",
                        "KeyPath": "",
                        "Passphrase": "UpKUJq1sD4Yfb1Hz8ZFiRw=="
                      },
                      "EnableAutoLogin": false,
                      "Host": "10.91.160.102",
                      "Password": "t7aoT+M7wIt7hzqlvPd+7g==",
                      "Port": "22",
                      "Protocol": "SFTP",
                      "TrustedPubKey": "",
                      "User": "drobinson"
                    },
                    "Transfer": {
                      "ASCIIFileExts": [
                        "TXT",
                        "INF",
                        "HTML",
                        "HTM"
                      ],
                      "ClearCommandChannel": false,
                      "ClearDataChannel": false,
                      "ConnectionTimeout": 30,
                      "CustomProxyCommands": [],
                      "DataPortMode": "AUTO",
                      "DelayBetweenRetries": 30,
                      "HomeIP": "0.0.0.0",
                      "HostName": "",
                      "MaxConcurrentThreads": 1,
                      "NumberOfConnectionRetries": 0,
                      "PASVPortMax": 65535,
                      "PASVPortMin": 0,
                      "Password": "UpKUJq1sD4Yfb1Hz8ZFiRw==",
                      "Port": 21,
                      "PreserveLocalTimeStamp": false,
```

```
      "PreserveRemoteTimeStamp": false,
      "ProxySeparator": "@",
      "ProxySubType": 0,
      "ProxyType": "FTP",
      "SOCKSSettings": {
        "Auth": false,
        "HostName": "",
        "Password": "UpKUJq1sD4Yfb1Hz8ZFiRw==",
        "Port": 1080,
        "Type": "None",
        "Use": false,
        "UserName": ""
      },
      "TransferEncoding": "UTF8",
      "UseProxy": false,
      "UserName": "",
      "ValidateFileIntegrity": false
    },
    "TransferAdditional": {
      "DeleteSourceIfMoveSkipped": true,
      "OverwriteType": "Overwrite",
      "PrePostCommandSettings": {
        "ContinueOnFailPost": false,
        "ContinueOnFailPre": false,
        "PostCommandArg": "",
        "PostCommandArgDelimiter": 32,
        "PostCommandType": "None",
        "PreCommandArg": "",
        "PreCommandType": "None"
      },
      "RenameDestinationFile": false,
      "RenameDestinationFileTo": "",
      "SyncSettings": {
        "SyncDeleteFileIfNotPresent": false,
        "SyncDirectionType": "MirrorRemote",
        "SyncFolders": false,
        "SyncIncludeSubfolders": false,
```

```
                    "SyncOverwriteType": "Overwrite"
                  },
                  "TreatMissingSourceAsSuccess": false
                }
              }
            }
          },
          "IfFailedActions": [
            {
              "StopAction": {
                "Enabled": false,
                "Result": "StopThisRule"
              }
            }
          ]
        },
        "ConditionStatement": {
          "Conditions": [],
          "ElseAttachedStatements": [],
          "IfAttachedStatements": [],
          "Operator": "Or"
        },
        "LoopDatasetStatement": {
          "Params": {
            "DatasetName": "",
            "EndLoopRow": 0,
            "OrderingColumn": "",
            "SortOrder": "Original",
            "StartLoopRow": 0,
            "UseEndLoopRow": false,
            "UseStartLoopRow": false
          },
          "Statements": []
        },
        "Type": "Action"
      }
    ],
```

```
          "Operator": "And"
        },
        "LoopDatasetStatement": {
          "Params": {
            "DatasetName": "",
            "EndLoopRow": 0,
            "OrderingColumn": "",
            "SortOrder": "Original",
            "StartLoopRow": 0,
            "UseEndLoopRow": false,
            "UseStartLoopRow": false
          },
          "Statements": []
        },
        "Type": "Condition"
      }
    ]
  },
  "trigger": {
    "TimerParams": {
      "DailyInfo": {
        "DayPeriod": 1,
        "EveryWeekDay": true
      },
      "EndDateEnabled": false,
      "EndDateTime": 1659710856,
      "EndTimeEnabled": false,
      "HolidayCalendarID": "00000000-0000-0000-0000-000000000000",
      "MonthlyInfo": {
        "DayPeriod": 1,
        "MonthPeriod": 1,
        "RelativeDay": "First",
        "UseFixedDayIndexInMonth": true,
        "Weekday": "Sunday"
      },
      "Recurrence": "Continually",
      "RepeatEnabled": true,
```

```
            "RepeatPattern": "Minutes",
            "RepeatRate": 8,
            "RundayCalendarID": "00000000-0000-0000-0000-000000000000",
            "StartDateTime": 1659710856,
            "WeeklyInfo": {
              "WeekDayFlags": 1,
              "WeekPeriod": 1
            },
            "YearlyInfo": {
              "DayPeriod": 1,
              "Month": "January",
              "RelativeDay": "First",
              "UseFixedDayIndexInFixedMonth": true,
              "Weekday": "Sunday"
            }
          }
        }
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$eventReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rules"
Method 'POST' -Headers $authHeader -Body $update
Write-Output $eventReturn | ConvertTo-Json
```

Endpoint: /sites/{siteid}/event-rules/{ruleid}

Get, modify, or delete a specific site event rule

- GET
- PATCH
- DELETE

Method & URL

```
GET https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rules/{ruleid}
```

GET Body Sample

GET Response Body Sample

GET PowerShell Sample

Method & URL

```
PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rules/{ruleid}
```

PATCH Body Sample

PATCH Response Body Sample

PATCH PowerShell Sample

Method & URL

```
DELETE https://[server URL]:[port]/admin/v2/sites/
{siteId}/event-rules/{ruleid}
```

DELETE Body Sample

DELETE Response Body Sample

DELETE PowerShell Sample

Endpoint: /sites/{siteid}/event-rule-folders

Get or create site event-rule-folders

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rule-folders

GET Body Sample

GET EVENT RULE FOLDER LIST

GET https://{{host}}/admin/v2/sites/{{Siteid}}/event-rule-folders HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###

GET Response Body Sample

{"data":[{"attributes":{"name":"<root>"},"id":"00000000-0000-0000-0000-000000000000","link":{"self":"/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/event-rule-folders/00000000-0000-0000-0000-000000000000"},"type":"eventRuleFolder"}],"links":{"self":"/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/event-rule-folders"}}

GET PowerShell Sample

Returns all site settings for the specified Site ID

User must obtain the SiteID from Get Sites

Write-Output "ER Folders"

Write-Output "----"

#$siteID = Enter SiteID here

$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-folders" -Method 'GET' -Headers $authHeader

```
Write-Output $siteList | ConvertTo-Json
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rule-folders

POST Body Sample

```
###

POST https://{{host}}/admin/v2/sites/{{Siteid}}/event-rule-folders HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

{

  "data":

  {

  "attributes": {

  "name": "Folder of user events"

  },

  "type": "eventRuleFolder"

  }

}

###
```

POST Response Body Sample

{"data":{"attributes":{"isRemote":false,"name":"Folder of user events"},"id":"38d270a9-6b40-4732-9942-5bdac9731d93","type":"eventRuleFolder"},"links":{"self":"/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/event-rule-folders/38d270a9-6b40-4732-9942-5bdac9731d93"}}

POST PowerShell Sample

```
##Patch SITE EVENT RULE FOLDER settings
```

```
Write-Output "Site Folder PATCH"

Write-Output "-----"

$update =

'{

  "data": {

    "attributes": {

      "isRemote": false,

      "name": "Folder of newer events"

    },

    "type": "eventRuleFolder"

  }

}'

$update = $update | ConvertFrom-Json

$update = $update | ConvertTo-Json -Depth 10

$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-
folders/$folderID" -Method 'PATCH' -Headers $authHeader -Body $update

Write-Output $patchReturn | ConvertTo-Json
```

Endpoint: /sites/{siteid}/event-rule-folders/{folderid}

Get, update, or delete a specific site event rule folder data

- GET
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rule-folders/{folderid}

GET Body Sample

###

@folderID = {{foldersList.response.body.$.data[0].id}}

GET https://{{host}}/admin/v2/sites/{{Siteid}}/event-rule-folders/{{folderID}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

###

GET Response Body Sample

HTTP/1.1 200 OKDate: Tue, 09 Aug 2022 17:23:43 GMTContent-Type: application/vnd.api+jsonETag: "98C84003"Content-Length: 255Cache-Control: no-cache, no-store, must-revalidateExpires: -1X-Content-Type-Options: nosniffX-XSS-Protection: 1; mode=blockContent-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;Referrer-Policy: no-referrer{"data": {"attributes": {"isRemote": false,"name": "<root>"},"id": "00000000-0000-0000-0000-000000000000","type": "eventRuleFolder"},"links": {"self": "/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/event-rule-folders/00000000-0000-0000-0000-000000000000"}}

GET PowerShell Sample

Write-Output "ER Folders"

Write-Output "----"

#$siteID = Enter SiteID here

```
$folderList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-folders" -Method 'GET' -Headers $authHeader

Write-Output $folderList | ConvertTo-Json

$folderID = $folderList.data[1].id

$foldersList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-folders/$folderID" -Method 'GET' -Headers $authHeader

Write-Output $foldersList | ConvertTo-Json
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rule-folders/{folderid}

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/event-rule-folders/{{folderID}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

{

  "data": {

    "attributes": {

      "isRemote": false,

      "name": "Folder of new events"

    },

    "type": "eventRuleFolder"

  }

}
```

PATCH Response Body Sample

HTTP/1.1 200 OKDate: Tue, 09 Aug 2022 18:07:40 GMTContent-Type: application/vnd.api+jsonETag: "1268DCC6"Content-Length: 269Cache-Control: no-

cache, no-store, must-revalidateExpires: -1X-Content-Type-Options: nosniffX-XSS-Protection: 1; mode=blockContent-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;Referrer-Policy: no-referrer{"data": {"attributes": {"isRemote": false,"name": "Folder of new events"},"id": "38d270a9-6b40-4732-9942-5bdac9731d93","type": "eventRuleFolder"},"links": {"self": "/admin/v2/sites/6203305a-d7c6-499e-a59b-81500765f8f2/event-rule-folders/38d270a9-6b40-4732-9942-5bdac9731d93"}}

PATCH PowerShell Sample

```
##Patch SITE EVENT RULE FOLDER settings

Write-Output "Site Folder PATCH"

Write-Output "-----"

$update =

'{

  "data": {

    "attributes": {

      "isRemote": false,

      "name": "Folder of newer events"

    },

    "type": "eventRuleFolder"

  }

}'

$update = $update | ConvertFrom-Json

$update = $update | ConvertTo-Json -Depth 10

$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-folders/$folderID" -Method 'PATCH' -Headers $authHeader -Body $update

Write-Output $patchReturn | ConvertTo-Json
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rule-folders/{folderid}

DELETE Body Sample

###

@folderID = {{foldersList.response.body.$.data[0].id}}

DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/event-rule-folders/{{folderID}} HTTP/1.1

Authorization: EFTAdminAuthToken {{AuthToken}}

DELETE Response Body Sample

HTTP/1.1 204 No ContentDate: Tue, 09 Aug 2022 18:12:00 GMTContent-Length: 0Cache-Control: no-cache, no-store, must-revalidateExpires: -1X-Content-Type-Options: nosniffX-XSS-Protection: 1; mode=blockContent-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;Referrer-Policy: no-referrer

DELETE PowerShell Sample

$folderID = $folderList.data[1].id

$folderList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-folders/$folderID" -Method 'DELETE' -Headers $authHeader

Write-Output $folderList | ConvertTo-Json

FORTRA

EFT REST API Reference

Copyright Terms and Conditions

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202301120854

Contents

Authentication REST API 6

Endpoint: /admin/v1/authentication 6

Server REST API 7

Endpoint: /server 7

Endpoint:/server/status 10

Endpoint: /server/metrics 11

Endpoint: /server/security/tls 13

Endpoint: /server/security/ssh 16

Endpoint: /server/reports 18

Endpoint: /server/admin-users 20

Endpoint: /server/admin-users/{adminId} 24

Endpoint: /server/admin-users-policy 27

Endpoint: /experimental/server/templates/{templateName} 30

Endpoint: /server/ha/upgrade 31

Endpoint:/server/admin/v2/authentication 33

Nodes REST API 34

Endpoint: /nodes 34

Endpoint: /nodes/{nodeId}/metrics 35

Endpoint: /nodes/{nodeId}/licenses 37

Endpoint: /nodes/{nodeId}/licenses/{moduleName} 40

Endpoint: /nodes/{nodeId}/licenses/trial-extension-challenge 41

Endpoint: /nodes/{nodeId}/licenses/trial-extension-response 41

Site REST API 42

Endpoint: /sites 42

Endpoint:/sites/status 44

Endpoint: /sites/{siteId} 45

Endpoint: /sites/{siteId}/metrics 47

Endpoint: /sites/{siteId}/authentication 49

Endpoint: /sites/{siteId}/general 53

Endpoint: /sites/{siteID}/ftps 56

Endpoint: /sites/{siteId}/https 59

Endpoint: /sites/{siteId}/networkAndSecurity 63

Endpoint: /sites/{siteId}/ipAccess 66
Endpoint: /sites/{siteId}/ipAccessList/{ipAccessId} 70
Endpoint: /sites/{siteId}/ipAutoBanList 73
Endpoint: /sites/{siteId}/ipAutoBanList/{ipAutoBanId} 74
Endpoint: /sites/{siteId}/sms 75
Endpoint: /sites/{siteId}/sms/{profileName} 77
Endpoint: /sites/{siteId}/accountSecurity 81
Endpoint: /sites/{ siteId}/workspaces 83
Endpoint: /sites/{siteId}/sendPortal 85
Endpoint: /sites/{ siteId}/dropOffPortal 88
Endpoint: /sites/{siteId}/privacyPolicy 91
Endpoint: /sites/{siteId}/termsOfService 93
Endpoint: /sites/{siteId}/gdpr 95
Endpoint: /sites/{siteId}/uploadForms 97
Endpoint: /sites/{siteId}/uploadForms/{uploadFormName} 99
Endpoint: /sites/{siteId}/userGroups 103
Endpoint: /sites/{siteId}/outlookDeploymentScript 104
Endpoint: /sites/{siteId}/contentIntegrity 104
Endpoint: /sites/{siteId}/contentIntegrity/{profileId} 107
Endpoint: /sites/{siteId}/custom-commands 110
Endpoint: /sites/{siteId}/custom-commands/{customCommandID} 113
Endpoint: /sites/{siteId}/user-templates 117
Endpoint: /sites/{siteId}/user-templates/{userTemplateid} 122
Endpoint: /sites/{siteId}/user-groups 129
Endpoint: /sites/{siteId}/user-groups/{groupid} 131
Endpoint: /sites/{siteId}/user-groups/{groupid}/relationships/users 134
Endpoint: /sites/{siteId}/ram/agents 138
Endpoint: /sites/{siteId}/ram/agents/{remoteAgentID} 139
Endpoint: /sites/{siteId}/ram/agents/templates 141
Endpoint: /sites/{siteId}/ram/agents/templates/{remoteAgentsTemplateID} 144
Endpoint:/sites/{siteId}/awe-tasks 148
Endpoint:/sites/{siteId}/awe-tasks/{aweTaskID} 151
Endpoint:/sites/{siteId}/awe-tasks-folders 154
Endpoint:/sites/{sitetId}/awe-tasks-folders/{aweTaskFolderID} 156

Endpoint: /sites/{siteId}/connection-profiles 160
Endpoint: /sites/{siteId}/connection-profiles/{connectionProfileID} 162
Endpoint: /experimental/site/templates/{templateName} 166
Endpoint:/sites/{siteID}/dmz 168
Security REST API 170
Endpoint: /lists/security/tls/algorithms 170
Endpoint: /lists/security/ssh/algorithms 171
Endpoint: /lists/security/tls/ciphers/{cipherString} 172
Login/Logout REST API 173
Endpoint: /logout 173
Keep-Alive REST API 173
Endpoint: /keep-alive 173
Users REST API 174
Endpoint: /sites/{siteId}/users 174
Endpoint: /sites/{siteid}/users/{userid} 177
Endpoint: /sites/{siteid}/users/{userid}/as2inbound 182
Endpoint: /sites/{siteid}/users/{userid}/as2outbound 184
Endpoint: /sites/{siteid}/users/{userid}/counters 187
Filesystem REST API 188
Endpoint: /sites/{siteId}/filesystem/folders 188
Endpoint: /sites/{siteId}/filesystem/folders/{folderid} 189
Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/folders 194
Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/permissions 196
Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/permissions/{folderpermid} 200
Event Rules REST API 204
Endpoint://sites/{siteid/event-rules 204
Endpoint: /sites/{siteid}/event-rules/{ruleid} 207
Endpoint:/sites/{siteid}/event-rule-folders 212
Endpoint:/sites/{siteid}/event-rule-folders/{folderid} 213

Authentication REST API

Endpoint: /admin/v1/authentication

Creates a session for the user and stores the authentication token. This token will be required for any subsequent REST API requests.

There are several supported Authentication types, EFT and AD. When using an Windows or AD account configure your authentication type to “AD” instead of “EFT”.

- POST

Method & URL

POST https://[server URL]:[port]/admin/v2/server

POST Body Sample

```
@host = 192.168.1.206:4450
@AdminUser = API_admin
@password = APIADMIN_Password!
###

# @name login
POST https://{{host}}/admin/v1/authentication HTTP/1.1
Content-Type: application/json

{"userName": "{{AdminUser}}", "password": "{{password}}",
"authType": "EFT"}
###
@AuthToken = {{login.response.body.$.authToken}}
###
```

POST Response Body Sample

```
HTTP/1.1 200 OK Date: Tue, 10 May 2022 14:02:47 GMT Content-
Type: application/vnd.api+json Content-Length: 215 Set-Cookie:
csrftoken=6FF1EF51-9771-E2EF-9227-79C73F660B20; path=/; secure;
SameSite=Lax Cache-Control: no-cache, no-store, must-revalidate
Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection: 1;
mode=block Content-Security-Policy: default-src 'self' 'unsafe-
inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer {
"authToken":
"95267D88A45EBA20B858CA8C4EB15B00F27F1FBBC6BC0B2F13DDE25889FF2C9
E", "permissions": [ { "policy": "ServerManagement" }, {
"policy": "COMManagement" }, { "policy": "ReportManagement" }, {
"policy": "ManagePersonalData" } ] }
```

POST PowerShell Sample

```
$baseURL = "https://192.168.100.165:4450/admin"
$AdminUser = "admin"
$password = "alaska"

# Only to ignore certificates errors
add-type @"
    using System.Net;
    using System.Security.Cryptography.X509Certificates;

        public class IDontCarePolicy : ICertificatePolicy {
        public IDontCarePolicy() {}
        public bool CheckValidationResult(
            ServicePoint sPoint, X509Certificate cert,
            WebRequest wRequest, int certProb) {
            return true;
        }
    }
"@
[System.Net.ServicePointManager]::CertificatePolicy = new-object
IDontCarePolicy
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12


# authentication
$authBody = "{""userName"": ""$AdminUser"", ""password"": ""$password"",
""authType"": ""EFT""}"
$auth = Invoke-RestMethod -Uri "$baseURL/v1/authentication" -Method 'POST' -
Body $authBody

$authToken = $auth.authToken
$authHeader = New-Object
"System.Collections.Generic.Dictionary[[String],[String]]"
$authHeader.Add("Authorization", "EFTAdminAuthToken $authToken")
```

Server REST API

Endpoint: /server

Returns and update server settings.

- GET

- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/server

GET Body Sample

```
GET https://{{host}}/admin/v2/server HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
"data": {
"type": "server",
"id": "1",
"attributes": {
 "version": "8.0.6.16",
 "general": {
  "configFilePath": "C:\\ProgramData\\Globalscape\\EFT  Server
Enterprise\\",
  "enableUtcInListings": true,
   "lastModifiedBy": "admin",
   "lastModifiedTime": 1633717057
  },
  "listenerSettings": {
   "adminPort": 1100,
   "enableRemoteAdministration": true,
    "listenIps": [ "0.0.0.0" ],
…

}
```


GET PowerShell Sample

```
#get Server
Write-Output "Get Server"
Write-Output "-----"
$serverDetails = Invoke-RestMethod -Uri "$baseURL/v2/server" -Method 'GET' -
Headers $authHeader
Write-Output $serverDetails | ConvertTo-Json
foreach ($server in $serverDetails.data)
{
    Write-Output ("Server $($serverDetails.data)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/server

PATCH Body Sample

```
PATCH  https://{{host}}/admin/v2/server HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
"data": {
    "type": "server",
    "id": "1",
    "attributes":{
        "version":"",
    "smtp": {
        "login": "",
        "password": "",
        "port": 587,
        "senderAddr": "EFT@mailserver.net",
        "senderName": "Globalscape EFT",
        "server": "smtp.mailserver.net",
        "useAuthentication": false,
        "useImplicitTLS": false
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

PATCH PowerShell Sample

```
##Patch Server - patching the SMTP settings
Write-Output "Server Patch"
Write-Output "-----"
$update =
'{
    "data":{
        "type": "server",
        "id": "1",
        "attributes": {
            "version": "",
        "smtp": {
            "login": "",
            "password": "",
            "port": 587,
            "senderAddr": "EFT@mailserver.net",
            "senderName": "Globalscape EFT",
            "server": "smtp.mailserver.net",
            "useAuthentication": false,
            "useImplicitTLS": false
         }
         }
     }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/server" -Method 'PATCH' -
Headers $authHeader -Body $update
```

Endpoint:/server/status

Returns server information

- GET

Method & URL

GET https://[server URL]:[port]/admin/v1/server/status

GET Body Sample

```
GET https://{{host}}/admin/v1/server/status HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

{"nodes":[{"activity":{"activeClientDownloadBytesPerSecond":0,"activeClientDownloadCount":0,"activeClientUploadBytesPerSecond":0,"activeClientUploadCount":0,"activeServerDownloadBytesPerSecond":0,"activeServerDownloadCount":0,"activeServerUploadBytesPerSecond":0,"activeServerUploadCount":0,"connectedAdminCount":1,"connectedUserCount":0,"runningAwTaskCount":0,"runningEventRuleCount":0},"isInCluster":false,"isMaster":false,"isStarted":true,"licenses":[{"module":"AAMModule","registrationState":"Evaluation period"},{"module":"ARMModule","registrationState":"Evaluation period"},{"module":"AS2Module","registrationState":"Evaluation period"},{"module":"AWModule","registrationState":"Evaluation

GET PowerShell Sample

```
#get Server Metrics
Write-Output "Get Server Metrics"
Write-Output "-----"
$serverMetrics = Invoke-RestMethod -Uri "$baseURL/v1/server/status" -Method
'GET' -Headers $authHeader
Write-Output $serverMetrics | ConvertTo-Json
foreach ($server in $serverMetrics.data)
{
    Write-Output ("Server $($serverMetrics.data)")
}
```

Endpoint: /server/metrics

Returns server metrics.

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/server/metrics

GET Body Sample

```
GET https://{{host}}/admin/v2/server/metrics HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
"data": {
  "type": "serverMetrics",
   "id": "1",
   "attributes": {
      "activeClientDownloadBytesPerSecond": 0,
       "activeClientDownloadCount": 0,
       "activeClientUploadBytesPerSecond": 0,
       "activeClientUploadCount": 0,
       "activeServerDownloadBytesPerSecond": 0,
       "activeServerDownloadCount": 0,
       "activeServerUploadBytesPerSecond": 0,
       "activeServerUploadCount": 0,
       "connectedAdminCount": 1,
       "connectedUserCount": 0,
       "runningAwTaskCount": 0,
       "runningEventRuleCount": 0
      }
    },
    "links": {
      "self": "admin/v2/server/metrics"
  }
}
```


GET PowerShell Sample

```
#get Server Metrics
Write-Output "Get Server Metrics"
Write-Output "-----"
$serverMetrics = Invoke-RestMethod -Uri "$baseURL/v2/server/metrics" -Method
'GET' -Headers $authHeader
Write-Output $serverMetrics | ConvertTo-Json
foreach ($server in $serverMetrics.data)
{
    Write-Output ("Server $($serverMetrics.data)")
}
```

Endpoint: /server/security/tls

Returns and updates server TLS security settings.

- Get
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/server/security/tls

GET Body Sample

```
GET https://{{host}}/admin/v2/server/security/tls HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
"data": {
  "type": "tlsServerSecuritySettings",
  "id": "1",
  "attributes": {
   "tlsSettings": {
      "minimumProtocolVersion": "TLSv1.3",
      "selectedAlgorithms":
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56:EECDH+CHACHA20:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3
DES:RSA+3DES:EECDH+RC4:RSA+RC4:!MD5:!SRP:!PSK:!EXP:!RC4:!SSLv3:!SHA1",
     "resultingCipherList":
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-
AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-
CCM8:ECDHE-ECDSA-AES128-CCM:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
SHA256:AES128-GCM-SHA256:AES128-CCM8:AES128-CCM:AES128-SHA256:ECDHE-
ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-
CCM8:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-
SHA384:AES256-GCM-SHA384:AES256-CCM8:AES256-CCM:AES256-SHA256",
     "manuallySelectedAlgorithms": {
       "enabled": false,
       "algorithms":
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56:EECDH+CHACHA20:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3
DES:RSA+3DES:EECDH+RC4:RSA+RC4:!MD5:!SRP:!PSK:!EXP:!RC4:!SSLv3:!SHA1"
     }
   },
   "tlsFipsEnabled": false
   } },
   "links": {
      "self": "admin/v2/server/security/tls"
   }
}
```


GET PowerShell Sample

```powershell
#get Server TLS Security Settings
Write-Output "Get Server TLS Settings"
Write-Output "-----"
$serverTLS = Invoke-RestMethod -Uri "$baseURL/v2/server/security/tls" -Method
'GET' -Headers $authHeader
Write-Output $serverTLS | ConvertTo-Json
foreach ($server in $serverTLS.data)
{
    Write-Output ("Server $($serverTLS.data)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/server/security/tls

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/server/security/tls HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "tlsServerSecuritySettings",
    "id": "1",
    "attributes": {
      "tlsFipsEnabled": true
    }
  },
  "links": {
    "self": "admin/v2/server/security/tls"
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

PATCH PowerShell Sample

```
###(PATCH) TLS Security Settings (enable FIPS)
Write-Output "Server TLS Enable FIPS Patch"
Write-Output "-----"
$update =
'{
 "data": {
    "type": "tlsServerSecuritySettings",
    "id": "1",
    "attributes": {
      "tlsFipsEnabled": true
    }
  },
  "links": {
    "self": "admin/v2/server/security/tls"
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/server/security/tls" -
Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /server/security/ssh

Returns and update server SSH security settings.

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/server/security/ssh

GET Body Sample

```
GET https://{{host}}/admin/v2/server/security/ssh HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
"data": {
  "type": "sshServerSecurity",
  "id": "1",
  "attributes": {
    "sshSettings": {
     "allowedCiphersList": "aes256-gcm@openssh.com,aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-gcm@openssh.com,aes128-ctr,aes128-cbc",
     "allowedKexesCiphersList": "ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group16-sha512,diffie-hellman-group14-sha256,diffie-hellman-group-exchange-sha256",
     "allowedMacsList": "hmac-sha2-512-etm@openssh.com,hmac-sha2-512,hmac-sha2-256-etm@openssh.com,hmac-sha2-256,hmac-sha1-etm@openssh.com,hmac-sha1",
     "softwareVersion": "8.1.0.0_openssh",
     "comments": "Globalscape"
    },
     "sshFipsEnabled": false
   }
 },
 "links": {
   "self": "admin/v2/server/security/ssh"
 }
}
```


GET PowerShell Sample

```
#get Server SSH Security Settings
Write-Output "Get Server SSH Settings"
Write-Output "-----"
$serverSSH = Invoke-RestMethod -Uri "$baseURL/v2/server/security/ssh" -Method 'GET' -Headers $authHeader
Write-Output $serverSSH | ConvertTo-Json
foreach ($server in $serverSSH.data)
{
    Write-Output ("Server $($serverSSH.data)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/server/security/ssh

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/server/security/ssh HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "sshServerSecurity",
    "id": "1",
    "attributes": {
      "sshFipsEnabled": true
    }
  },
  "links": {
    "self": "admin/v2/server/security/ssh"
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

PATCH PowerShell Sample

```
###(PATCH) SSH Security Settings (enable FIPS)
Write-Output "Server SSH Enable FIPS Patch"
Write-Output "-----"
$update =
'{
 "data": {
    "type": "sshServerSecurity",
    "id": "1",
    "attributes": {
      "sshFipsEnabled": true
    }
  },
  "links": {
    "self": "admin/v2/server/security/ssh"
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/server/security/ssh" -
Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /server/reports

Returns the DPIA and PCI-compliance reports in JSON format.

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/server/reports/DPIA

GET Body Sample

```
GET https://{{host}}/admin/v2/server/reports/DPIA HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
"data": {
  "attributes": {
    "dpia": [ {
        "articles": [ {
            "desc": "The processing of personal data falls within Article 2's definition of material scope. Risk is increased only if set to unknown scope.",
            "name": "Material scope",
            "num": 2,
            "score": 1,
            "value": "Unknown or undefined" }, {
            "desc": "Specifies the territorial scope your organization has identified in context with this application's usage.",
            "name": "Territorial scope",
            "num": 3,
            "score": 1,
            "value": "Unknown or undefined" }, {
            "desc": "If Not in Union was chosen for territorial scope then all users must have their data subject status set to either Yes or No.",


…
  }
```


GET PowerShell Sample

```powershell
#get Server DPIA Report
Write-Output "Get Server DPIA Report"
Write-Output "-----"
$serverDPIA = Invoke-RestMethod -Uri "$baseURL/v2/server/reports/DPIA" -Method
'GET' -Headers $authHeader
Write-Output $serverDPIA | ConvertTo-Json -Depth 20
foreach ($server in $serverDPIA.data)
{
    Write-Output ("Server $($serverDPIA.data)")
}
```

Method & URL

(Please note this is a V1 endpoint)

GET https://[server URL]:[port]/admin/v1/server/reports/PCICompliance

GET Body Sample

```
GET https://{{host}}/admin/v1/server/reports/PCICompliance HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
HTTP/1.1 200 OK Date: Tue, 09 Aug 2022 17:30:22 GMT Content-Type:
application/vnd.api+json Content-Length: 234 Cache-Control: no-cache, no-
store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-
Protection: 1; mode=block Content-Security-Policy: default-src 'self'
'unsafe-inline' 'unsafe-eval'
data:; Referrer-Policy: no-referrer { "PCICompliance": [ { "failed": 12,
"passed": 12, "siteId": "e82de253-b8ec-4b70-a72d-d017c3317f01",
"siteName": "MySite", "warnings": 6 }, { "failed": 6, "passed": 11, "siteId":
"ff493a39-1e28-40c5-ab18-2e6a4f33f296", "siteName": "PCI_SITE",
"warnings": 5 } ] }
```


GET PowerShell Sample

```powershell
#get Server PCIC Report
Write-Output "Get Server PCIC Report"
Write-Output "-----"
$serverPCIC = Invoke-RestMethod -Uri
"$baseURL/v1/server/reports/PCICompliance" -Method 'GET' -Headers $authHeader
Write-Output $serverPCIC | ConvertTo-Json -Depth 20
foreach ($server in $serverPCIC.data)
{
    Write-Output ("Server $($serverPCIC.data)")
}
```

Endpoint: /server/admin-users

Returns list of EFT admin users and creates new admin users.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/server/admin-users

GET Body Sample

```
GET https://{{host}}/admin/v2/admin-users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
"data": [
 {
    "id": "59774c12-870d-5560-a44a-c5b35cf68d4c",
  "type": "adminUser",
  "attributes": {
   "name": "admin"
  }
 },
 {
  "id": "b76a1d7b-c3ad-5ac4-8636-06ce71ba3af3",
  "type": "adminUser",
  "attributes": {
   "name": "Local computer\\Administrators"
  }
 }
 ],
 "links": {
  "self": "admin/v2/admin-users"
 }
}
```

GET PowerShell Sample

```
#get Server admin users
Write-Output "Get Server admin users"
Write-Output "-----"
$serverAdmins = Invoke-RestMethod -Uri "$baseURL/v2/admin-users" -Method
'GET' -Headers $authHeader
Write-Output $serverAdmins | ConvertTo-Json
foreach ($server in $serverAdmins.data)
{
    Write-Output ("Server $($serverAdmins.data)")
}
```

Method & URL

POST https://[server URL]:[port]/admin/v2/server/admin-users

POST Body Sample

```
POST https://{{host}}/admin/v2/admin-users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
 "data":{
   "attributes":{
   "name":"Test_admin2",
   "password":"test",
   "adminConsolePermissions":{
    "accountPolicy":"server",
    "enableCom":true,
    "enableEditingAndReporting":true,
    "enablePersonalDataAccess":true
   },
   "restPermissions":{
    "enabled":true,
    "restAdminRole":true
   }
  }
 }
}
```

POST Response Body Sample

```
HTTP/1.1 201 Created Date: Tue, 09 Aug 2022 18:18:00 GMT Content-Type:
application/vnd.api+json ETag: "BF7E8C0E" Content-Length: 394 Cache-
Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-
Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy:
no-referrer

{ "data":

{ "id": "9693cbcf-d4a9-49ac-aa1c-59efd91a692b", "type": "adminUser",
"attributes": { "adminConsolePermissions": { "accountPolicy": "Server",
"enableCom": true, "enableEditingAndReporting": true,
"enablePersonalDataAccess": true }, "name": "Test_admin2",
"restPermissions": { "enabled": true, "restAdminRole":
"server_full_access" } } }, "links": { "self": "/admin/v2/admin-
users/9693cbcf-d4a9-49ac-aa1c-59efd91a692b" } }
```

POST PowerShell Sample

```
#POST Server Admin user (New User)
Write-Output "POST Server Admin (New Admin user)"
Write-Output "-----"
$update =
'{
  "data": {
    "id": "1",
    "attributes": {
      "name": "Test_admin",
      "password": "test",
      "adminConsolePermissions": {
        "accountPolicy": "server",
        "enableCom": true,
        "enableEditingAndReporting": true,
        "enablePersonalDataAccess": true
      },
      "restPermissions": {
        "enabled": true,
        "restAdminRole": true
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/admin-users" -Method
'POST' -Headers $authHeader -Body $update
```

Endpoint: /server/admin-users/{adminId}

Returns EFT admin user (adminID required) information, which allows PATCH (update) and DELETE of admin user. To obtain the admin user ID a GET request will need to be done against the /admin-users endpoint prior to making this REST API request.

- GET
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/server/admin-users/{adminID}

GET Body Sample

```
GET https://{{host}}/admin/v2/admin-users/59774c12-870d-5560-a44a-
c5b35cf68d4c HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
"data": {
  "id": "59774c12-870d-5560-a44a-c5b35cf68d4c",
  "type": "adminUser",
  "attributes": {
    "adminConsolePermissions": {
      "accountPolicy": "Server",
      "enableCom": true,
      "enableEditingAndReporting": true,
      "enablePersonalDataAccess": true
    },
    "name": "admin",
    "restPermissions": {
      "enabled": true,
      "restAdminRole": "server_full_access"
    }
  }
 },
 "links": {
   "self": "admin/v2/admin-users/59774c12-870d-5560-a44a-c5b35cf68d4c"
 }
}
```


GET PowerShell Sample

```
#Get Server Admin Details when providing a Server Admin ID
Write-Output "Get Server Admin Details"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/admin-
users/59774c12-870d-5560-a44a-c5b35cf68d4c" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($server in $serverAdminDetails.data)
{
    Write-Output ("Server $($serverAdminDetails.data)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/server/admin-users/{adminID}.

PATCH Body Sample

```
@adminID = 13564c1b-8e13-4e72-b8e0-9480fad06221
PATCH https://{{host}}/admin/v2/admin-users/{{adminID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "0",
    "attributes": {
        "adminConsolePermissions": {
        "enableCom": false,
        "enableEditingAndReporting": true,
        "enablePersonalDataAccess": true
      },
      "restPermissions": {
        "enabled": true,
        "restAdminRole": true
      }
    }
  }
}
```

PATCH PowerShell Sample

```
###
#PATCH Server Admin Details when providing a Server Admin ID
Write-Output "Server Admin User Patch"
$adminID = "13564c1b-8e13-4e72-b8e0-9480fad06221"
Write-Output "Admin ID: $adminID"
Write-Output "-----"
$update =
'{
  "data": {
    "id": "0",
    "attributes": {
        "adminConsolePermissions": {
        "enableCom": false,
        "enableEditingAndReporting": true,
        "enablePersonalDataAccess": true
      },
      "restPermissions": {
        "enabled": true,
        "restAdminRole": true
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/admin-users/$adminID" -
Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/server/admin-users/{adminID}.

DELETE Body Sample

```
@adminID = 13564c1b-8e13-4e72-b8e0-9480fad06221
DELETE https://{{host}}/admin/v2/admin-users/{{adminID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE PowerShell Sample

```
###
#DELETE EFT admin by Admin ID
Write-Output "Server Admin DELETE"
$adminID = "f98d2a35-4d37-4891-89ed-66cb6ddf9436"
Write-Output "Admin ID: $adminID"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/admin-
users/$adminID" -Method 'DELETE' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($server in $serverAdminDetails.data)
{
    Write-Output ("Server $($serverAdminDetails.data)")
}
```

Endpoint: /server/admin-users-policy

Returns EFT admin user policies such as account and password policy. Additionally, the PATCH request allows updates to the EFT admin policies.

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/server/admin-users-policy

GET Body Sample

```
GET https://{{host}}/admin/v2/admin-users-policy HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": {
      "id": "1",
      "type": "adminUserPolicy",
      "attributes": {
        "accountPolicy": {
          "invalidLogin": {
            "account": {
              "enabled": false,
              "attemptPeriodMinutes": 5,  "attemptRetries": 5,
"lockoutMinutes": 30 }}, "inactivity": { "disconnectDueToTimeout": {
"enabled": false,   "timeoutMinutes": 5},"removeInactiveAccounts":
{"enabled": false,  maxInactiveDays": 90}}},   "passwordPolicy": {
"complexity": {           "enabled": false,           "minLength": 8,
"userNameSimilarity": {            "enabled": true,
"maxAllowedChars": 3 }, "repeatingCharLimit": { "enabled": true,
"maxAllowedChars": 3 }, "characterCategories": { "enabled": true,
"characterCount": 4, "numericRequired": true, "upperCaseRequired": true,
"lowerCaseRequired": true, "nonAlphaNumericRequired": false,
"non7bitAsciiRequired": false }, "forbiddenDictionary": { "enabled":
true, "backwardsWordsAllowed": false, "dictionaryFilePath": "" } },
"forceResetAfterFirstLogin": false, "history": { "enabled": false,
"historyDepth": 4 }, "reset": { "expiration": { "enabled": false,
"daysToExpire": 90 } } } } }, "links": { "self": "admin/v2/admin-users-
policy" } }
```


GET PowerShell Sample

```
###
#GET Server Admin user policy
Write-Output "Get Server Admin User Policy"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/admin-users-policy"
-Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($server in $serverAdminDetails.data)
{
    Write-Output ("Server $($serverAdminDetails.data)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/server/admin-users-policy

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/admin-users-policy HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "1",
    "type": "adminUserPolicy",
    "attributes": {
      "accountPolicy": {
          "inactivity": {
          "disconnectDueToTimeout": {
            "enabled": false,
            "timeoutMinutes": 5
          }

        }
      }
    }
  }
}
```

PATCH PowerShell Sample

```
###
#PATCH Server Admin user policy (disable Admin UI disconnect)
Write-Output "Server Admin User Policy Patch"
Write-Output "-----"
$update =
'{
  "data": {
    "id": "1",
    "type": "adminUserPolicy",
    "attributes": {
      "accountPolicy": {
          "inactivity": {
          "disconnectDueToTimeout": {
            "enabled": false,
            "timeoutMinutes": 5
          }

        }
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/admin-users-policy" -Method
'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /experimental/server/templates/{templateName}

Note: Available as of EFT 8.1.0

Returns and updates the contents of the specified server template.

- GET
- PATCH

Method & URL

GET HTTPS://{{host}}/admin/experimental/server/templates/{templateName}

GET Body Sample

```
#GET Server Templates -- ##
GET
https://{{host}}/admin/experimental/server/templates/WorkspacesAdminAddedParticipantMsg.html HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 13:17:16 GMT Content-Type: application/vnd.api+json Content-Length: 370 Cache-Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer { "data": "<html>\r\n<body>\r\n <p>Hello %USER.LOGIN%,</p>\r\n <p>The following <b>Enhanced File Transfer</b> Workspace has been shared with you: %FOLDER_NAME% (owner: %WS_OWNER_NAME%).</p>\r\n <p>Please use the following URL to access this Workspace:</p>\r\n <a href=\"%LINK%\">%LINK%</a><br/><br/>\r\n \r\n %WS_MESSAGE%<br/><br/>\r\n <hr/>\r\n</body>\r\n</html>" }
```


GET PowerShell Sample

```
####################################
#GET Server Templates -- ##
Write-Output "GET Server Templates Detail"
Write-Output "------------------------------"
#$siteID = "Enter site ID"
#$TemplateName= "WorkspacesAdminAddedParticipantMsg.html"
$TemplateDetails = Invoke-RestMethod -Uri "$baseURL/experimental/server/templates/WorkspacesAdminAddedParticipantMsg.html" -Method 'GET' -Headers $authHeader
Write-Output $TemplateDetails | ConvertTo-Json -Depth 25
```

Method & URL

PATCH HTTPS://{{host}}/admin/experimental/server/templates/{templateName}

PATCH Body Sample

```
###
#PATCH - Update Server template ###
PATCH
https://{{host}}/admin/experimental/server/templates/PasswordResetReminderMsg.html
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": "<html>\r\n<body>\r\n HELLO USERS %USER.FULL_NAME%,<br>\r\nThe -___API
TEST___ password for account: %USER.LOGIN% will expire in %DAYS_LEFT% days. Please
change your password at your earliest convenience.\r\nInstructions for changing your
password via FTP, SFTP, and HTTP/S are provided below for your convenience:<br>\r\n1.
Please enter the following URL into your browser:
%SITE.ACCOUNT_MANAGEMENT_URL%<br>\r\n2. Supply your current password when
prompted<br>\r\n3. Enter your new password and confirm<br>\r\n4. If approved, exit the
browser and login as normal<br>\r\n</body>\r\n</html>"
}
```

PATCH PowerShell Sample

```
### Update Content of Template###
### Modify Server Template - ###
Write-Output "PATCH Server Template"
Write-Output "--------------------"
$update =
'
{
  "data":  "Notice: ___PATCH TEST__The SSL certificate: %certid% is set to expire %d% day(s)
from now on %expirationdate%, which may impact operations or communications with the
entity associated with this certificate."
}
'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$TemplateDetails = Invoke-RestMethod -Uri
"$baseURL/experimental/server/templates/SSLCertExpirationWarning.txt" -Method 'PATCH' -
Headers $authHeader -Body $update
```

Endpoint: /server/ha/upgrade

Note: Available as of EFT 8.1.0

The GET request returns node HA upgrade state. Additionally, the POST request changes the entire HA cluster state to the upgrade or normal state.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/server/ ha/upgrade

GET Body Sample

```
### GET server upgrade state ###
GET https://{{host}}/admin/v2/server/ha/upgrade HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": "notInUpgrade" }
```

GET PowerShell Sample

```
#########
#Get Server Upgrade State
Write-Output "Get Server Upgrade State: "
Write-Output "-----"
$upgradeState = Invoke-RestMethod -Uri "$baseURL/v2/server/ha/upgrade" -Method
'GET' -Headers $authHeader
Write-Output $upgradeState | ConvertTo-Json -Depth 10
```

Method & URL

POST https://[server URL]:[port]/admin/v2/server/ ha/upgrade

POST Body Sample

```
### "Normal" state -> "Upgrade" state ###
POST https://{{host}}/admin/v2/server/ha/upgrade HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data":
    {
        "action":"begin"
    }
}
###
```

POST PowerShell Sample

```
###
#POST Server Upgrade State to “begin”
Write-Output "Server Upgrade State POST"
Write-Output "-----"
$update =
'{
    "data":
    {
        "action":"begin"
    }
}'
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/server/ha/upgrade" -Method
'POST' -Headers $authHeader -Body $update
```

Endpoint:/server/admin/v2/authentication

Note: Available as of EFT 8.1.0

Return info about admin session

- GET

Method & URL

GET https://{{host}}/admin/v2/authentication

GET Body Sample

```
###
GET https://{{host}}/admin/v2/authentication HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

{"data":{"authToken":"1B1EFBE3D705EEAABC6404F3E1705C46C93E9962C6DA618A8EE534133A81C097","idleTimeoutMinutes":1,"username":"admin"}}

GET PowerShell Sample

```
# authentication
$authBody = "{""userName"": ""$AdminUser"", ""password"": ""$password"",
""authType"": ""EFT""}"
$auth = Invoke-RestMethod -Uri "$baseURL/v1/authentication" -Method 'POST' -
Body $authBody

$authToken = $auth.authToken
$authHeader = New-Object
"System.Collections.Generic.Dictionary[[String],[String]]"
$authHeader.Add("Authorization", "EFTAdminAuthToken $authToken")

# keep-alives
Write-Output "administration metrics"
Write-Output "----"
for( $count = 0; $count -lt 10; $count++) {
   $adminInfo = Invoke-RestMethod -Uri "$baseURL/v2/authentication" -Method
'GET' -Headers $authHeader
   Write-Output $adminInfo
   }
```

Nodes REST API

Endpoint: /nodes

Returns a list of EFT Nodes.

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/nodes

GET Body Sample

```
GET https://{{host}}/admin/v2/nodes HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
  "data": [
    {
      "type": "node",
      "id": "WIN-4NFJASSP163",
      "links": {
        "metrics": "admin/v2/nodes/WIN-4NFJASSP163/metrics"
      },
      "attributes": {
        "isStarted": true,
        "isInCluster": false,
        "fullDomainName": "WIN-4NFJASSP163",
        "version": "8.0.7.4",
        "hostIps": [
          "127.0.0.1",
          "fe80::351a:6044:dfe2:f53%2"
        ] } } ], "links": { "self": "admin/v2/nodes/" } }
```


GET PowerShell Sample

```
###
#GET SERVER NODES
Write-Output "Get EFT Server Nodes"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/nodes" -Method 'GET'
-Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($server in $serverAdminDetails.data)
{
    Write-Output ("Server $($serverAdminDetails.data)")
}
```

Endpoint: /nodes/{nodeId}/metrics

Returns an EFT server's metrics, including transfers and server status. To obtain the node ID a GET request will need to be done against the /nodes endpoint prior to making this REST API request.

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/nodes/{nodeID}/metrics

GET Body Sample

```
GET https://{{host}}/admin/v2/nodes HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "type": "nodeMetrics",
    "id": "WIN-4NFJASSP163",
    "attributes": {
      "activity": { "activeClientDownloadBytesPerSecond": 0,
      "activeClientDownloadCount": 0,
      "activeClientUploadBytesPerSecond": 0,
      "activeClientUploadCount": 0,
      "activeServerDownloadBytesPerSecond": 0,
      "activeServerDownloadCount": 0,
      "activeServerUploadBytesPerSecond": 0,
      "activeServerUploadCount": 0,
      "connectedAdminCount": 1,
      "connectedUserCount": 0,
      "runningAwTaskCount": 0,
      "runningEventRuleCount": 0
     },
      "isInCluster": false, "isMaster": false, "isStarted": true,
```


GET PowerShell Sample

```
###
#GET SERVER NODE METRICS
Write-Output "Get EFT Server Node Metrics"
$serverNodeID = "WIN-4NFJASSP163"
Write-Output "Server Node ID: $serverNodeID"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri
"$baseURL/v2/nodes/$serverNodeID/metrics" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($server in $serverAdminDetails.data)
{
    Write-Output ("Server $($serverAdminDetails.data)")
}
```

Endpoint: /nodes/{nodeId}/licenses

Returns list of licenses on an EFT node and provides the ability to register EFT or a module.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/nodes/{nodeId}/licenses

GET Body Sample

```
@NodeID = WIN-4NFJASSP163
GET https://{{host}}/admin/v2/nodes/{{NodeID}}/licenses HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
"data": [
  {
    "attributes": {
      "registrationStatus": "Evaluation period"
    },
    "id": "AAMModule",
    "links": {
      "self": "admin/v2/nodes/WIN-4NFJASSP163/licenses/AAMModule"
    },
     "type": "license" }, { "attributes": { "registrationStatus":
"Evaluation period" }, "id": "ARMModule", "links": { "self":
"admin/v2/nodes/WIN-4NFJASSP163/licenses/ARMModule" }, "type": "license"
},
```


GET PowerShell Sample

```
###
#GET SERVER NODE LICENSE
Write-Output "Get EFT Server Node Licenses"
$serverNodeID = "WIN-4NFJASSP163"
Write-Output "Server Node ID: $serverNodeID"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri
"$baseURL/v2/nodes/$serverNodeID/licenses" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Method & URL

POST https://[server URL]:[port]/admin/v2/nodes/{nodeId}/licenses

POST Body Sample

```
@NodeID = WIN-4NFJASSP163
POST https://{{host}}/admin/v2/nodes/{{NodeID}}/licenses HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": [
    {
      "id": "ARMModule",
      "attributes": {
        "serialNumber": "MySerialNumberHere"
      }
    }
  ]
}
```

POST PowerShell Sample

```
###
#POST SERVER NODE LICENSE
Write-Output "Register EFT Server Node"
$serverNodeID = "WIN-4NFJASSP163"
Write-Output "Server Node ID: $serverNodeID"
Write-Output "-----"
$update =
'{
  "data": [
    {
      "id": "ARMModule",
      "attributes": {
        "serialNumber": "MySerialNumberHere"
      }
    }
  ]
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/nodes/$serverNodeID/licenses" -Method 'POST' -Headers $authHeader
-Body $update
```

Available options for ids:

- AAMModule (Advanced Authentication Modes)
- ARMModule (Auditing and Reporting Module)
- AS2Module (Applicability Statement 2 Module)
- AWModule (Advanced Workflow Engine Module)
- AccelerateModule (FAST Protocol – ***Deprecated***)
- CloudConnectorModule (CCM – Cloud Connector Module)
- DMZGWModule (DMZ Gateway Module)
- EFTServer (EFT Server)
- EnterpriseActionsWModule (Enterprise Actions Module)
- FTPModule (FTP/S Module)

- FileTransferClientModule (File Transfer Client Module)
- FolderMonitorEventModule (Folder Monitor Event Module)
- HSModule (*will be deprecated*)
- HTTPModule (HTTP/s Module)
- PGPModule (OpenPGP Module)
- RAModule (Remote Agent Module)
- SSHModule (SFTP Module)
- SecureFormsModule (Secure Forms Module)
- TimerEventModule (Timer Event Module)
- WorkspacesModule (Workspaces Module)

Endpoint: /nodes/{nodeId}/licenses/{moduleName}

Returns registration status of a given module

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/nodes/{nodeId}/licenses/{moduleName}

GET Body Sample

```
###
#GET Module Registration Status
@moduleName = EFTServer
GET https://{{host}}/admin/v2/nodes/{{NodeId}}/licenses/{{moduleName}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "attributes": { "registrationState": "Evaluation period" },
"id": "EFTServer", "type": "license" }, "links": { "self":
"admin/v2/nodes/DTY2019WinServe/licenses/EFTServer" } }
```

GET PowerShell Sample

```
###
#GET A SERVER NODE LICENSE MODULE INFORMATION
Write-Output "Get EFT Server Node Licenses"
$serverNodeID = "DTY2019WinServe"
$licenseModule = "EFTServer"

Write-Output "License Module: $licenseModule"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri
"$baseURL/v2/nodes/$serverNodeID/licenses/$licenseModule" -Method 'GET' -
Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Endpoint: /nodes/{nodeId}/licenses/trial-extension-challenge

Returns trial extension challenge string

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/nodes/{nodeId}/licenses/trial-extension-challenge

GET Body Sample

```
###
#GET TRIAL EXTENSION CHALLENGE
@NodeID = “DTY2019WinServe”
GET https://{{host}}/admin/v2/nodes/{{NodeId}}/licenses/trial-extension-challenge HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "attributes": { "challengeString": "nnPwL0AAq2304GWn0KnniO0z85owwH6xL3vw8pQm0LvdUVE10=" }, "id": "1", "type": "trialExtension" }, "links": { "self": "admin/v2/licenses/trial-extension-challenge" } }
```

GET PowerShell Sample

```
###
#GET TRIAL EXTENSION CHALLENGE
Write-Output "Get EFT Server Node Licenses"
$serverNodeID = "DTY2019WinServe"

Write-Output "$serverNodeID"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/nodes/$serverNodeID/licenses/trial-extension-challenge" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Endpoint: /nodes/{nodeId}/licenses/trial-extension-response

Allows the user to provide response string to extend the trial.

- POST

Method & URL

POST https://[server URL]:[port]/admin/v2/nodes/{nodeId}/licenses/trial-extension-response

POST Body Sample

```
@NodeID = "DY-Win2019-1a"

POST https://{{host}}/admin/v2/nodes/{{NodeID}}/licenses/trial-extension-response HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
      "responseString":
"XN00P00PSJ00P00PUD00P00PK02JZLM3RJM7968J3LKKKQ01VWZVBU3VLXMXKF03VNLMXAJO
LOKKWONYUE3COMNQV8KE2JFEO6YNQ3KZT3AU3RMOTBJXU0MLUE3UQELK3JOM1JN8L3XOS3TNY
KE2TL7NJ3TKWMTLZJ0XP00PT8WE5TWETUFK39TB396UDMTM5VW1VM3PSWTQV9TKE1TQ3P6JEI
2KE7VUE0TKW2TO6WTWTKEZTWE3W7TUF3RKFW3M3PS83PS03PS03RCPSB3RCPS83RCT"
    }
  }
}
###
```

POST Response Body Sample

```
HTTP/1.1 200 OK Date: Tue, 09 Aug 2022 22:17:23 GMT Content-Type: application/vnd.api+json Content-Length: 212 Cache-Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer {
"data": { "attributes": { "response": "Trial Extended! Your new trial END date is 8/24/2022." }, "id": "1", "type": "trialExtension" }, "links": {
"self": "/admin/v2/nodes/\"DY-Win2019-1a\"/licenses/trial-extension-response" } }
```

Site REST API

Endpoint: /sites

Returns and update site(s) settings.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites

GET Body Sample

```
### GET SITE ###
# @name siteList

GET https://{{host}}/admin/v2/sites HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{ "data": [ { "type": "site", "id": "892b16dc-24a8-473f-a74e-
c597b824c879", "attributes": { "name": "MySite" }, "links": { "self":
"admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879", "metrics":
"admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879/metrics" } },

{ "type": "site", "id": "5f99540a-da95-41c4-8b3c-d423848bdd46",
"attributes": { "name": "MySite2" }, "links": { "self":
"admin/v2/sites/5f99540a-da95-41c4-8b3c-d423848bdd46", "metrics":
"admin/v2/sites/5f99540a-da95-41c4-8b3c-d423848bdd46/metrics" } } ],
"links": { "self": "admin/v2/sites" } }
```


GET PowerShell Sample

```
# Get all sites
Write-Output "Site"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites" -Method 'GET' -
Headers $authHeader
Write-Output $siteList | ConvertTo-Json
foreach ($site in $siteList.data)
{
    Write-Output ("Site  $($site.id): $($site.attributes.name)")
}

$siteID = $siteList.data[0].id
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites

POST Body Sample

```
#POST Create a new Site
POST https://{{host}}/admin/v2/sites HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "site",
    "attributes": {
      "pciComplianceEnabled": true,
      "siteLabel": "MySite5",
      "siteRootFolder": "C:\\InetPub\\EFTRoot\\MySite\\",
      "createUnixStyleSubFolders": true,
      "createFoldersForNewUsers": true
    }
  }
}
```

POST Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated POST request(s).

POST PowerShell Sample

```
####Added 2/01/2020
#POST Site/ (Create a new Site)
Write-Output "POST Site (Create a new Site)"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "site",
    "attributes": {
      "pciComplianceEnabled": true,
      "siteLabel": "MySite6",
      "siteRootFolder": "C:\\InetPub\\EFTRoot\\MySite\\",
      "createUnixStyleSubFolders": true,
      "createFoldersForNewUsers": true
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites" -Method 'POST' -
Headers $authHeader -Body $update
```

Endpoint:/sites/status

Returns the current status of all sites

- GET

Method & URL

GET https://[server URL]:[port]/admin/v1/sites/status

GET Body Sample

```
### GET SITE ###
# @name siteList

GET https://{{host}}/admin/v1/sites/status HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

{"info":[{"nodeName":"DY-Win2019-1a","sites":[{"DMZConnected":false,"activity":{"activeClientDownloadBytesPerSecond":0,"activeClientDownloadCount":0,"activeClientUploadBytesPerSecond":0,"activeClientUploadCount":0,"activeServerDownloadBytesPerSecond":0,"activeServerDownloadCount":0,"activeServerUploadBytesPerSecond":0,"activeServerUploadCount":0,"connectedUserCount":0,"runningAWTaskCount":0,"runningEventRuleCount":0},"id":"5ceae6e3-11b1-40c6-b4e4-3078a8e88a35","lastUserLoginTime":0,"name":"MySite","startTime":1659543775,"state":"Running"}]}]}

GET PowerShell Sample

```
# Get all sites
Write-Output "Site"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v1/sites/status" -Method 'GET' -
Headers $authHeader
Write-Output $siteList | ConvertTo-Json
foreach ($site in $siteList.data)
{
    Write-Output ("Site  $($site.id): $($site.attributes.name)")
}
```

Endpoint: /sites/{siteId}

Returns all site settings for the specified Site ID; To obtain the Site ID a GET request will need to be done against the /sites endpoint prior to making this request.

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteid}

GET Body Sample

```
### Returns all site settings for the specified Site ID ###
GET https://{{host}}/admin/v2/sites/{{Siteid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
      "type": "site",
      "id": "892b16dc-24a8-473f-a74e-c597b824c879",
      "attributes": { "name": "MySite",
      "general": { "authType": "EFT",
       "rootFolder": "C:\\InetPub\\EFTRoot\\MySite\\",
       "lastModifiedBy": "WIN-IKTLG8MULV9\\Administrator",
       "lastModifiedTime": 1643636803
      },
      "listenerSettings": {
       "accountManagementUrl": "https://172.22.150.62/manageaccount",
       "httpDomain": "172.22.150.62",
       "listenIps": [ "0.0.0.0" ],
       "ftps": { "explicitPort": 21,
       "implicitPort": 990 },
       "https": { "port": 443 },
       "sftp": { "port": 22 } },
       "workspacesSettings": { "enabled": true },
       "dmz": { "enabled": false,
       "server": [ { "nodeName": "WIN-IKTLG8MULV9",
       "ipAddresses": [ "" ],
       "port": 44500 } ] } } },
       "links": { "metrics": "admin/v2/sites/892b16dc-24a8-473f-a74e-
      c597b824c879/metrics",
      "self": "admin/v2/sites/892b16dc-24a8-473f-a74e-c597b824c879" }
      }
```


GET PowerShell Sample

```
####Added 2/01/2020
### Returns all site settings for the specified Site ID ###
### User must obtain the SiteID from Get Sites
Write-Output "Site"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID" -Method 'GET' -
Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/metrics

Returns all site metrics for the specified Site ID; To obtain the Site ID a GET request will need to be done against the /sites endpoint prior to making this request.

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteid}/metrics

GET Body Sample

```
### GET Site Metrics ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/metrics/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "id": "4d1b02ee-5c9c-4129-bf1d-663534248b3f",
    "type": "siteMetrics",
    "attributes": {
      "name": "MySite6",
      "startTime": " 12:00:00 AM",
      "isRunning": false,
      "isDMZGatewayConnected": false,
      "definedUsers": 0,
      "disabledUserCount": 0,
      "nodes": [
        {
          "activeClientDownloadBytesPerSecond": 0,
          "activeClientDownloadCount": 0,
          "activeClientUploadBytesPerSecond": 0,
          "activeClientUploadCount": 0,
          "activeServerDownloadBytesPerSecond": 0,
          "activeServerDownloadCount": 0,
          "activeServerUploadBytesPerSecond": 0,
          "activeServerUploadCount": 0,
          "connectedUserCount": 0,
          "name": "WIN-IKTLG8MULV9",
          "runningAWTaskCount": 0,
          "runningEventRuleCount": 0
        }
      ]
    }
```

GET PowerShell Sample

```
### Returns all site Metrics for the specified Site ID ###
### User must obtain the SiteID from Get Sites
Write-Output "Site Metrics"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/metrics" -Method
'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/authentication

Returns current authentication settings for the Site ID specified on the request; To obtain the Site ID a GET request will need to be done against the /sites endpoint prior to making this request.

- GET
- PATCH

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteid}/authentication

GET Body Sample

```
### GET Site Authentication Provider (EFT, AD, LDAP, ODBC) ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/authentication/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "id": "3e2cae3a-db0f-44bd-812d-4ca6b0f04c91",
    "type": "siteAuthentication",
    "attributes": {
      "advancedAuth": {},
      "userAuth": {
        "type": "LDAP",
        "ldap": {
          "advanced": {
            "ldapVersion": {
              "enabled": true,
              "version": 3
            },
            "overrideSearchPage": {
              "enabled": true,
              "size": 1000
            },
            "referralChasingEnabled": false,
            "searchScope": {
              "enabled": true,
              "level": 2
            },
            "serverSidePageControlEnabled": true,
            "timeOut": {
              "enabled": true,
              "seconds": 60
            },
```

GET PowerShell Sample

```
####Added 2/02/2022
### GET Site Authentication Provider (EFT, AD, LDAP, ODBC) ###
### User must obtain the SiteID from Get Sites
Write-Output "Site Authentication Provider "
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/authentication"
-Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteid}/authentication

PATCH Body Sample

```
###This example will Set ODBC as the Authentication type and enable
radius
#PATCH Site Authentication type
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/authentication/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
  "data": {
    "id": "",
    "type": "site",
    "attributes": {
      "userAuth": {
        "type": "ODBC",
        "odbc": {
          "connectionString":
"Provider=MSDASQL;SERVER=;DATABASE=ODBC;UID=sa;PWD= ",
          "encryptUserPassword": true,
          "refreshInterval": {
            "inherited": true,
            "enabled": false,
            "minutes": 0
          }
        }
      },
      "advancedAuth": {
        "type": "radius",
        "radius": {
          "server": "",
          "port": 0,
          "nasIdentifier": "",
          "sharedSecret": "",
          "connectionRetries": 0,
```

GET Response Body Sample


```
{
  "data": {
    "id": "c4d4bf76-2172-41e7-9ed1-3c2d0de1254c",
    "type": "siteAuthentication",
    "attributes": {
      "advancedAuth": {
        "type": "radius",
        "radius": {
          "connectionRetries": 0,
          "nasIdentifer": "",
          "port": 0,
          "server": "",
          "sharedSecret": "",
          "timeOutSeconds": 0
        }
      },
      "userAuth": {
        "type": "ODBC",
        "odbc": {
        "connectionString":
"Provider=MSDASQL;SERVER=;DATABASE=ODBC;UID=sa;PWD=",
          "encryptUserPassword": true,
          "refreshInterval": {
            "inherited": true,
            "enabled": 0,
            "minutes": 0
          }
        }
```

PATCH PowerShell Sample

```
### PATCH Site Authentication Provider (EFT, AD, LDAP, ODBC) ###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH Site Authentication Provider"
Write-Output "-----"
$update =
'{
  "data": {
    "id": "",
    "type": "site",
    "attributes": {
      "userAuth": {
        "type": "ODBC",
        "odbc": {
          "connectionString":
"Provider=MSDASQL;SERVER=192.168.100.70;DATABASE=ODBC;UID=sa;PWD=alaska",
          "encryptUserPassword": true,
          "refreshInterval": {
            "inherited": true,
            "enabled": false,
            "minutes": 0
          }
        }
      },
      "advancedAuth": {
        "type": "radius",
        "radius": {
          "server": "",
          "port": 0,
          "nasIdentifier": "",
          "sharedSecret": "",
          "connectionRetries": 0,
          "timeOutSeconds": 0
        }
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/authentication" -Method 'PATCH' -Headers
$authHeader -Body $update
```

Endpoint: /sites/{siteId}/general

Returns and update the site general settings.

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/general

GET Body Sample

```
### GET Site General Settings ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/general/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "type": "siteGeneral",
    "attributes": {
      "overrideVfsCredentials": {
        "enabled": false,
        "value": {
          "login": "",
          "password": ""
        }
      },
      "siteRootFolder":  "C:\\InetPub\\EFTRoot\\MySite\\"
    }
  },
  "links": {
    "self": "/admin/v2/sites/892b16dc-24a8-473f-a74e-
c597b824c879/general"
  }
}
```


GET PowerShell Sample

```
### GET Site General Settings###
### User must obtain the SiteID from Get Sites
Write-Output "Site General Settings"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/general" -Method
'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Note: As of EFT 8.1.0 the general REST API endpoint will also return any VFS Site Root folder configuration details when the site root has been configured in the cloud.

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/general

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/general/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "",
    "type": "",
    "attributes": {
      "siteRootFolder": "C:\\InetPub\\EFTRoot\\MySite\\",
      "overrideVfsCredentials": {
        "enabled": true,
        "value": {
          "login": "test",
          "password": "passwordtest"
        }
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
{
  "data": {
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "type": "siteGeneral",
    "attributes": {
      "overrideVfsCredentials": {
        "enabled": true,
        "value": {
          "login": "test",
          "password": "cGFzc3dvcmR0ZXN0"
        }
      },
```

PATCH PowerShell Sample

```
### PATCH Site General Settings###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH Site General Settings"
Write-Output "-----"
$update =
'{
  "data": {
    "id": "",
    "type": "",
    "attributes": {
      "siteRootFolder": "C:\\InetPub\\EFTRoot\\MySite\\",
      "overrideVfsCredentials": {
        "enabled": true,
        "value": {
          "login": "test",
          "password": "passwordtest"
        }
      }
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/general" -
Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteID}/ftps

Returns and update the FTP(s) settings

- GET

- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ftps

GET Body Sample

```
### GET Site FTP(s) Settings ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ftps/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "type": "site",
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "attributes": {
      "ftp": {
        "enabled": false,
        "port": 21
      },
      "explicitFtps": {
        "enabled": true,
        "port": 21
      },
      "implicitFtps": {
        "enabled": true,
        "port": 990
      },
      "ftpConfig": {
        "enableClearCommandChannel": false,
        "enableFtpClientAntiTimeout": true,
```


GET PowerShell Sample

```
### GET Site FTP(S) Settings###
### User must obtain the SiteID from Get Sites
Write-Output "Site FTP(S) Settings"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ftps" -Method
'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/general

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/ftps/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes":{
      "ftp": {
        "enabled": true,
        "port": 10
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
{
  "data": {
    "type": "site",
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "attributes": {
      "ftp": {
        "enabled": true,
        "port": 10
      },
      "explicitFtps": {
        "enabled": true,
        "port": 10
      },
      "implicitFtps": {
```

PATCH PowerShell Sample

```
### PATCH FTP(S) Settings###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH FTP(S) Settings"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes":{
      "ftp": {
        "enabled": true,
        "port": 25
      }
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ftps" -Method
'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/https

Returns and update the HTTP(s) settings

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/https

GET Body Sample

```
### GET Site HTTP(s) Settings ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/https/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "type": "site",
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "attributes": {
      "http": {
        "enabled": false,
        "port": 80
      },
      "https": {
        "enabled": true,
        "port": 411
      },
      "domain": "172.22.150.62",
      "enableRestPage": false,
      "redirectHttpToHttps": false,
      "enableHsts": true,
      "allowWebServices": false,
      "as2": {
        "enabled": false,
```


GET PowerShell Sample

```
### GET Site HTTP(s) Settings###
### User must obtain the SiteID from Get Sites
Write-Output "Site HTTPS(S) Settings"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/https" -Method
'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/https

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/https/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes":{
      "https": {
        "enabled": true,
        "port": 490
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
{
  "data": {
    "type": "site",
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "attributes": {
      "http": {
        "enabled": false,
        "port": 80
      },
      "https": {
        "enabled": true,
        "port": 490
      },
      "domain": "172.22.150.62",
      "enableRestPage": false,
      "redirectHttpToHttps": false,
      "enableHsts": true,
      "allowWebServices": false,
      "as2": {
        "enabled": false,
```

PATCH PowerShell Sample

```
### PATCH  Site HTTP(s) Settings###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH  Site HTTP(s) Settings"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes":{
      "https": {
        "enabled": true,
        "port": 25
      }
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/https" -
Method 'PATCH' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/networkAndSecurity

Returns and update the network and security settings.

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/networkandsecurity/

GET Body Sample

```
### GET Site Network and Security Settings ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/networkandsecurity/
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
  "data": {
    "type": "site",
    "id": "892b16dc-24a8-473f-a74e-c597b824c879",
    "attributes": {
      "connectionLimits": {
        "maxTransferSpeed": false,
        "maxConcurrentSocketConnections": false,
        "maxConcurrentLogins": false,
        "maxConnectionsPerUser": false,
        "maxConnectionFromSameIP": false
      },
      "autoBan": {
        "enabled": true,
        "value": {
          "banIfExcessiveInvalidCmdsReceived": true,
          "banIpsPermanently": false,
          "numberOfInvalidCmds": 5,
          "sensitivityLevel": "Medium"
        }
```


GET PowerShell Sample

```
####Added 2/03/2022
### GET Site Network and Security Settings###
### User must obtain the SiteID from Get Sites
Write-Output "GET Site Network and Security Settings"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/networkandsecurity" -Method 'GET' -Headers
$authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/1networkandsecurity/

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/networkandsecurity/
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
      "connectionLimits": {
        "maxConcurrentLogins": true,
        "maxConcurrentSocketConnections": true,
        "maxConnectionFromSameIP": true,
        "maxConnectionsPerUser": true,
        "maxTransferSpeed": true
      },
      "denialOfService": {
        "autoBan": {
          "enabled": true,
          "value": {
            "banIfExcessiveInvalidCmdsReceived": true,
            "numberOfInvalidCmds": true,
            "sensitivityLevel": "Low",
            "banIpsPermenantly": true
          }
        }
      }
    }
  }
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
HTTP/1.1 200 OK Date: Thu, 25 Aug 2022 18:58:06 GMT Content-Type:
application/vnd.api+json ETag: "88131696" Content-Length: 663 Cache-
Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-
Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy:
no-referrer { "data": { "type": "site", "id": "c9551b5d-f904-4612-b690-
d51bfde2eb1f", "attributes": { "connectionLimits": { "maxTransferSpeed":
true, "maxTransferSpeedValue": 820, "maxConcurrentSocketConnections":
true, "maxConcurrentSocketConnectionsValue": 10, "maxConcurrentLogins":
true, "maxConcurrentLoginsValue": 10, "maxConnectionsPerUser": true,
"maxConnectionsPerUserValue": 1, "maxConnectionFromSameIP": true,
"maxConnectionFromSameIPValue": 1 }, "autoBan": { "enabled": true,
"value": { "banIfExcessiveInvalidCmdsReceived": true,
"banIpsPermanently": false, "numberOfInvalidCmds": 5, "sensitivityLevel":
"Medium" } } } }, "links": { "self": "/admin/v2/sites/c9551b5d-f904-4612-
b690-d51bfde2eb1f/networkAndSecurity" } }
```

PATCH PowerShell Sample

```
##Patch SITE Network Security settings
Write-Output "Site Network Security PATCH"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes": {
      "connectionLimits": {
        "maxConcurrentLogins": true,
        "maxConcurrentSocketConnections": true,
        "maxConnectionFromSameIP": true,
        "maxConnectionsPerUser": true,
        "maxTransferSpeed": true
      },
      "denialofService": {
        "autoBan": {
          "enabled": true,
          "value": {
            "banIfExcessiveInvalidCmdsReceived": true,
            "numberOfInvalidCmds": true,
            "sensitivityLevel": "Low",
            "banIpsPermenantly": true
          }
        }
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchNSReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/networkandsecurity" -Method 'PATCH' -Headers
$authHeader -Body $update
Write-Output $patchNSReturn | ConvertTo-Json
```

Endpoint: /sites/{siteId}/ipAccess

Returns and update the network and security Site IP access/ban list Settings.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ipAccessList

GET Body Sample

```
### GET Site IP access/ban list Settings ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ipAccessList HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
  "data": [
    {
      "id": "192.168.100.*",
      "type": "access",
      "attributes": {
        "accessType": "Allow",
        "date": "2022-02-04",
        "isAutoBan": false,
        "reason": "Allow for test",
        "sequenceNumber": 1
      }
    },
    {
      "id": "0.0.0.0",
      "type": "access",
      "attributes": {
        "accessType": "Deny",
        "date": "1969-12-31",
        "isAutoBan": true,
```


GET PowerShell Sample

```
### GET Site IP access/ban list Settings###
### User must obtain the SiteID from Get Sites
Write-Output "GET Site IP access/ban list Settings"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ipAccessList" -
Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/ipAccessList

POST Body Sample

```
POST https://{{host}}/admin/v2/sites/{{Siteid}}/ipAccessList HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "139:10:112:56::246",
    "type": "access",
    "attributes": {
      "accessType": "Allow",
      "reason": "API TEST",
      "sequenceNumber": 4
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).

```
{
  "data": {
    "id": "139:10:112:56::246",
    "type": "access",
    "attributes": {
      "accessType": "Allow",
      "date": "2022-02-04",
      "isAutoBan": false,
      "reason": "API TEST",
      "sequenceNumber": 4
    }
  },
  "links": {
    "self": "/admin/v2/sites/a70ccebd-1317-4992-84e7-
bb4cbddc02e4/ipAccessList/139:10:112:56::246"
  }
}
```

PATCH PowerShell Sample

```
### POST Site IP access/ban list Settings###
### User must obtain the SiteID from Get Sites
Write-Output "POST Site IP access/ban list Settings"
Write-Output "-----"
$update =
'
{
  "data": {
    "id": "139:10:112:57::246",
    "type": "access",
    "attributes": {
      "accessType": "Allow",
      "reason": "API TEST",
      "sequenceNumber": 5
    }
  }
}
'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ipAccessList"
-Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/ipAccessList/{ipAccessId}

Returns, update and deletes network and security Site IP access/ban list Settings for the specified IP.

- GET
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ipAccessList/ipAccessId

GET Body Sample

```
### GET Site IP access/ban Settings For specific IP###
GET
https://{{host}}/admin/v2/sites/{{Siteid}}/ipAccessList/{{ipAccessId}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
  "data": {
    "id": "139:10:112:56::246",
    "type": "access",
    "attributes": {
      "accessType": "Allow",
      "date": "2022-02-04",
      "isAutoBan": false,
      "reason": "API TEST",
      "sequenceNumber": 2
    }
  },
  "links": {
    "self": "/admin/v2/sites/a70ccebd-1317-4992-84e7-
bb4cbddc02e4/ipAccessList/139:10:112:56::246"
  }
}
```


GET PowerShell Sample

```
####Added 2/07/2022
### GET Site IP access/ban Settings For specific IP ###
### User must obtain the SiteID from Get Sites
Write-Output "GET Site IP access/ban list Settings For specific IP "
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ipAccessList/$ipAccessId" -Method 'GET' -Headers
$authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/ipAccessList/ipAccessList/{ipAccessId}

PATCH Body Sample

```
## PATCH Site Network and Security Settings For specific IP###
PATCH
https://{{host}}/admin/v2/sites/{{Siteid}}/ipAccessList/{{ipAccessId}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "139:10:112:56::247",
    "attributes": {
      "accessType": "Allow",
      "reason": "This is a test for API PATCH on IP",
      "sequenceNumber": 2
    }
  }
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).


```
{ "data": { "id": "139:10:112:56::247", "type": "access", "attributes": {
"accessType": "Allow", "date": "2022-02-07", "isAutoBan": false,
"reason": "This is a test for API PATCH on IP", "sequenceNumber": 2 } },
"links": { "self": "/admin/v2/sites/a70ccebd-1317-4992-84e7-
bb4cbddc02e4/ipAccessList/139:10:112:56::247" } }
```


PATCH PowerShell Sample

```
### PATCH Site Network and Security Settings For specific IP###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH Site Network and Security Settings For specific IP"
Write-Output "-----"
$update =
'{
  "data": {
    "id": "139:10:112:56::247",
    "attributes": {
      "accessType": "Allow",
      "reason": "This is a test for PS PATCH on IP",
      "sequenceNumber": 2
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 9
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ipAccessList/$ipAccessId" -Method 'PATCH' -Headers
$authHeader -Body $update
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/ipAccessList/{ipAccessId}

DELETE Body Sample

```
### DELETE Site IP access/ban Settings For specific IP###
DELETE
https://{{host}}/admin/v2/sites/{{Siteid}}/ipAccessList/{{ipAccessId}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Tue, 09 Aug 2022 20:34:49 GMT Content-
Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1 X-
Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-
Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
####Added 2/07/2022
### DELETE Site IP access/ban Settings For specific IP ###
### User must obtain the SiteID from Get Sites
### User must obtain the IP id to be deleted ###
Write-Output "DELETE Site IP access/ban Settings For specific IP ###"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ipAccessList/$ipAccessId" -Method 'DELETE' -Headers
$authHeader
Write-Output $siteList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/ipAutoBanList

Returns information about the Auto-banned Ips list

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ipAutoBanList

GET Body Sample

```
### GET Autoban List###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ipAutoBanList HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{"data":[{"id":"10.91.160.139","type":"accessBan"}],"links":{"self":"/adm
in/v2/sites/5ceae6e3-11b1-40c6-b4e4-3078a8e88a35/ipAutoBanList"}}
```


GET PowerShell Sample

```
$siteID = $siteList.data[0].id


####Added 2/01/2020
### Returns all site auto ban list###
Write-Output "Site Auto Ban List"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/IpAutoBanList" -
Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/ipAutoBanList/{ipAutoBanId}

Remove a specific IP from the Auto-banned IP list

- DELETE

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/ipAccessList{ipAutoBanId)

DELETE Body Sample

```
@banId = {{banList.response.body.$.data[0].id}}


### GET Autoban List###
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/ipAutoBanList/{{banId}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content
Date: Thu, 04 Aug 2022 19:43:37 GMT
Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate
Expires: -1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
$banID = $banList.data[0].id

$banList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/IpAutoBanList/$banID" -Method 'DELETE' -Headers
$authHeader
Write-Output $banList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/sms

Returns and updates the SMS configuration for the site.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/sms

GET Body Sample

```
### GET SMS Configuration####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/sms HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
  "data": [
    {
      "id": "Twilio Generic",
      "type": "smsSettings",
      "attributes": {
        "serviceType": "twilioGeneric",
        "services": {
          "accountSid": "xxxxxxx ...",
          "authToken": "xxxxx ....",
          "twilioNumber": "+1210...",
          "message": "Your passcode is: %Account_Session_OTP%",
          "postUrl": "https://api.twilio.com/2010-04-
01/Accounts/%SID%/Messages"
        },
```

GET PowerShell Sample

```
####Added 2/08/2022 ###
###GET SMS Settings for Site###
Write-Output "GET SMS Settings for Site"
Write-Output "----"
#$siteID = "Enter site ID"
$smsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sms" -Method
'GET' -Headers $authHeader
Write-Output $smsList | ConvertTo-Json -Depth 25
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/sms

POST Body Sample

```
### POST add an SMS profile###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/sms HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
      "name": "Test Post SMS",
      "serviceType": "genericSmsProviderProfile",
      "services": {
        "accountSid": "AAAAAAAAAAAAAAAAAAAAAAe",
        "authToken": "0dddd0dddd0dddd0dddd",
        "twilioNumber": "+1210210210",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-
01/Accounts/%SID%/Messages"
      },
      "proxy": {
        "enabled": true,
        "type": "192.168.100.100",
        "hostName": "testproxy",
        "port": 1443,
        "userName": "",
        "password": ""
      }
    `
```

POST Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated POST request(s).


```
{
  "data": {
    "id": "Test Post SMS",
    "type": "smsSettings",
    "attributes": {
      "name": "Test Post SMS",
      "serviceType": "twilioGeneric",
      "services": {
        "accountSid": "AAAAAAAAAAAAAAAAAAAAAAe",
        "authToken":  "0dddd0dddd0dddd0dddd",
```


POST PowerShell Sample

```
### POST add a new SMS profile ###
### User must obtain the SiteID from Get Sites
Write-Output "add a new SMS profile "
Write-Output "----------------------"
$update =
'{
  "data": {
    "attributes": {
      "name": "PowerShell Example",
      "serviceType": "genericSmsProviderProfile",
      "services": {
        "accountSid": "AAAAAAAAAAAAAAAAAAAAAe",
        "authToken": "0dddd0dddd0dddd0dddd",
        "twilioNumber": "+1210210210",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
      },
      "proxy": {
        "enabled": true,
        "type": "192.168.100.100",
        "hostName": "testproxy",
        "port": 1443,
        "userName": "TestUser",
        "password": "example"
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 25
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sms" -Method
'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/sms/{profileName}

Returns, updates and deletes the SMS configuration for specific profile.

- GET
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/sms/{profileName}

GET Body Sample

```
### GET SMS Configuration####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/sms/{profileName} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{
  "data": {
    "id": "Test Post SMS",
    "type": "smsSettings",
    "attributes": {
      "name": "Test Post SMS",
      "serviceType": "twilioGeneric",
      "services": {
        "accountSid": "AAAAAAAAAAAAAAAAAAAAAAe",
        "authToken": "0dddd0dddd0dddd0dddd",
        "twilioNumber": "+1210210210",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-
```


GET PowerShell Sample

```
####Added 2/08/2022 ###
###GET specific profile SMS Configuration Details###
Write-Output "GET specific profile SMS Configuration Details"
Write-Output "----"
$profileName = "PowerShell Example"
$smsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sms/$profileName"
-Method 'GET' -Headers $authHeader
Write-Output $smsList | ConvertTo-Json -Depth 25
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/sms/{profileName}

PATCH Body Sample

```
### PATCH SMS specific profile ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/sms/{{profileName}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
      "name": "",
      "serviceType": "genericSmsProviderProfile",
      "services": {
        "accountSid": "43243243214324234321FDGFDSG",
        "authToken": "1234567899",
        "twilioNumber": "210101010101",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-
01/Accounts/%SID%/Messages"
      }
    }
  }
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).


```
{
  "data": {
    "id": "Test Post SMS",
    "type": "smsSettings",
    "attributes": {
      "name": "Test Post SMS",
      "serviceType": "twilioGeneric",
      "services": {
        "accountSid": "43243243214324234321FDGFDSG",
        "authToken": "1234567899",
        "twilioNumber": "210101010101",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-
```

PATCH PowerShell Sample

```
####Added 2/08/2022
### PATCH - Updates existing SMS profile ###
### User must obtain the SiteID from Get Sites
Write-Output "add a new SMS profile "
Write-Output "----------------------"
$profileName = "PowerShell Example"
$update =
'{
  "data": {
    "attributes": {
      "name": "",
      "serviceType": "genericSmsProviderProfile",
      "services": {
        "accountSid": "43243243214324234321FDGFDSG",
        "authToken": "1234567899",
        "twilioNumber": "210101010101",
        "message": "Your passcode is: %Account_Session_OTP%",
        "postUrl": "https://api.twilio.com/2010-04-01/Accounts/%SID%/Messages"
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 25
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/sms/$profileName" -Method 'PATCH' -Headers
$authHeader -Body $update
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/sms/{profileName}

DELETE Body Sample

```
### DELETE SMS specific profile###
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/sms/{{profileName}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
{ "data": [ { "id": "Twilio Generic", "type": "smsSettings",
"attributes": { "serviceType": "twilioGeneric", "services": {
"accountSid": "Aabdd54dgsb2e9357b03a", "authToken":
```

DELETE PowerShell Sample

```
###### DELETE SMS specific profile######
Write-Output "### DELETE SMS specific profile###"
Write-Output "----"
$profileName = "PowerShell Example"
$smsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sms/$profileName"
-Method 'DELETE' -Headers $authHeader
Write-Output $smsList | ConvertTo-Json -Depth 25
```

Endpoint: /sites/{siteId}/accountSecurity

Returns and updates account security configuration for specific profile

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/sms/accountSecurity

GET Body Sample

```
### GET Account Security Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/accountSecurity/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{
  "data": {
    "type": "siteSecurity",
    "id": "0de7387f-1506-427d-b997-e18bcdb8cbae",
    "attributes": {
      "accountPolicy": {
        "invalidLogin": {
          "ip": {
            "enabled": true,
            "attemptPeriodMinutes": 1,
            "attemptRetries": 5,
```

GET PowerShell Sample

```
####Added 2/09/2022 ###
### GET Account Security Configuration Details ###
Write-Output "GET Account Security Configuration Details"
Write-Output "----"
$profileName = "PowerShell Example"
$smsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/accountSecurity"
-Method 'GET' -Headers $authHeader
Write-Output $smsList | ConvertTo-Json -Depth 25
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/sms/accountSecurity

PATCH Body Sample

```
### PATCH Account Security Settings ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/accountSecurity/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
  "data": {
    "attributes": {
      "accountPolicy": {
        "invalidLogin": {
          "account": {
            "enabled": true,
            "action": "Lockout",
            "attemptPeriodMinutes": 10,
            "attemptRetries": 10,
            "lockoutMinutes": 10
          },
          "ip": {
            "enabled": true,
            "attemptPeriodMinutes": 10,
            "attemptRetries": 10,
            "inCorrectLoginType": "NameOrPassword"
          }
        },
        "inactivity": {
          "removeInactiveAccounts": {
            "enabled": true,
            "action": "Delete",
            "maxInactiveDays": 10
          }
        },
        "reset": {
          "enabled": true,
          "forceResetAfterFirstLogin": true,
          "expiration": {
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).

```
{ "data": { "type": "site", "id": "0de7387f-1506-427d-b997-e18bcdb8cbae",
```

PATCH PowerShell Sample

```
### PATCH Account Security Configuration Details ###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH Account Security Configuration Details"
Write-Output "----------------------"
$update =
'{
  "data": {
    "attributes": {
      "accountPolicy": {
        "invalidLogin": {
          "account": {
            "enabled": true,
            "action": "Disable",
            "attemptPeriodMinutes": 3,
            "attemptRetries": 3,
            "lockoutMinutes": 3
```

Endpoint: /sites/{ siteId}/workspaces

Returns and updates workspaces settings

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/workspaces/

GET Body Sample

```
### GET Workspaces - Folder Sharing Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/workspaces/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
"data": { "type": "workspaces", "id": "0de7387f-1506-427d-b997-
e18bcdb8cbae", "attributes": { "enabled": true, "newUser": { "enabled":
true, "allowedDomains": { "enabled": false, "list": [ "*.*" ] },
"deniedDomains": { "enabled": false, "list": [ "*.*" ] } },
"maxExpiration": { "value": 1, "units": "Year" }, "secondVerification":
"email", "guestAccounts": { "expiration": { "enabled": true, "action":
"DeleteAccountOnly", "daysAfterLinksExpiration": 7 }, "grantHomeFolder":
true } } }, "links": { "self": "admin/v2/sites/0de7387f-1506-427d-b997-
e18bcdb8cbae/workspaces" } }
```

GET PowerShell Sample

```
###GET workspaces Configuration Details###
Write-Output "GET workspaces Configuration Details"
Write-Output "----"
#$siteID = "Enter site ID"
$wksList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/workspaces" -
Method 'GET' -Headers $authHeader
Write-Output $wksList | ConvertTo-Json -Depth 25
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/workspaces

PATCH Body Sample

```
### PATCH Workspaces - Folder Sharing Setting ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/workspaces/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
      "enabled": true,
      "newUsers": {
        "enabled": true,
        "allowedDomains": {
          "enabled": false
        }
      }
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).

```
HTTP/1.1 200 OK Date: Thu, 25 Aug 2022 19:20:16 GMT Content-Type:
application/vnd.api+json ETag: "FC63C399" Content-Length: 507 Cache-
Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-
Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy:
no-referrer { "data": { "type": "workspaces", "id": "c9551b5d-f904-4612-
b690-d51bfde2eb1f", "attributes": { "enabled": true, "newUsers": {
"enabled": true, "allowedDomains": { "enabled": false, "list": [ "*.*" ]
}, "deniedDomains": { "enabled": false, "list": [ "*.*" ] } },
"maxExpiration": { "value": 1, "units": "Year" }, "secondVerification":
"email", "guestAccounts": { "expiration": { "enabled": false, "action":
"Disable", "daysAfterLinksExpiration": 7 }, "grantHomeFolder": false } }
}, "links": { "self": "/admin/v2/sites/c9551b5d-f904-4612-b690-
d51bfde2eb1f/workspaces" } }
```

PATCH PowerShell Sample

```
##Patch SITE Workspaces settings
Write-Output "Site Workspaces PATCH"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes": {
      "enabled": true,
      "newUsers": {
        "enabled": true,
        "allowedDomains": {
          "enabled": false
        }
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchWSReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/workspaces"
-Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $patchWSReturn | ConvertTo-Json
```

Endpoint: /sites/{siteId}/sendPortal

Returns and updates send portal configuration for specific site

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/sendPortal

GET Body Sample

```
### GET Send Portal Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/sendPortal/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type":
"sendPortal", "attributes": { "enabled": true, "recipients":
"UsersGuestsAnonymous", "allowedDomains": { "enabled": false, "list": [
"*.*" ] }, "deniedDomains": { "enabled": false, "list": [ "*.*" ] },
"reservedPath": "/send", "protocol": "https", "hostName":
"172.31.223.227", "port": "443", "autoAttachInOutlook": { "enabled":
```


GET PowerShell Sample

```
###GET Send Portal Configuration Details###
Write-Output "GET Send Portal Configuration Details"
Write-Output "-------------------------------------"
#$siteID = "Enter site ID"
$SendList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/sendPortal" -
Method 'GET' -Headers $authHeader
Write-Output $Sendlist | ConvertTo-Json -Depth 25
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/sendPortal

PATCH Body Sample

```
### PATCH Send Portal Settings ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/sendPortal/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "sendPortal",
    "attributes": {
      "enabled": true,
      "recipients": "UsersGuestsAnonymous",
      "allowedDomains": {
        "enabled": true,
        "list": [
          "hotmail.*", "gmail.*"
        ]
      },
      "deniedDomains": {
        "enabled": true,
        "list": [
          "GSB.*"
        ]
      },
      "reservedPath": "/send",
      "protocol": "https",
      "hostName": "172.31.223.227",
      "port": "443",
      "autoAttachInOutlook": {
        "enabled": false,
        "whenExceedMbytes": 10
      },
      "linkExpiration": {
        "value": 1,
        "units": "Month"
      },
      "retainFilesAfterLinkExpiration": {
        "value": 0,
        "unit": "Day"
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type":
"sendPortal", "attributes": { "enabled": true, "recipients":
"UsersGuestsAnonymous", "allowedDomains": { "enabled": false, "list": [
"hotmail.*", "gmail.*" ] }, "deniedDomains": { "enabled": false, "list":
[ "GSB.*" ] }, "reservedPath": "/send", "protocol": "http", "hostName":
"", "port": "113", "autoAttachInOutlook": { "enabled": false,
"whenExceedMbytes": 10 }, "linkExpiration": { "value": 1, "units":
"Month" }, "retainFilesAfterLinkExpiration": { "value": 0, "unit": "Day"
}, "allowRepliesWithFiles": true, "sendEntireMessageSecurely":
"LetUserChoose", "outOfBandPasscode": "Sender chooses",
"secondVerification": "email", "fileRequestPortal": { "enabled": false,
"reservedPath": "/request" } } }, "links": { "self":
"/admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/sendPortal" } }
```


PATCH PowerShell Sample

```
Write-Output "PATCH Send Portal Configuration Details"
Write-Output "---------------------------------------"
$update =
'{
  "data": {
    "type": "sendPortal",
    "attributes": {
      "enabled": true,
      "recipients": "UsersGuestsAnonymous",
      "allowedDomains": {
        "enabled": true,
        "list": [
          "outlook.*", "yahoo.*"
        ]
      },
      "deniedDomains": {
        "enabled": true,
        "list": [
          "GSB.*"
        ]
```

Endpoint: /sites/{ siteId}/dropOffPortal

Returns and updates drop off portal configuration for specific site

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/dropOffPortal

GET Body Sample

```
## GET Drop Off Portal Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/dropOffPortal/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{ "data": { "id": "df3be28b-f499-4b0a-9c53-7cee33a58161",
"type": "dropOffPortal", "attributes": { "enabled": true,
"reservedPath": "/dropoff", "captcha": { "type": "reCAPTCHA",
"value": { "siteKey": "6LeXY8ofdsfdsfdsfasq8RdygpeBeclHqrVBUd-
afar", "secretKey": "6LeXY8oUAAAAABIVq8RdygpeBeclHqrVBUd-afar" }
}, "linkExpiration": { "value": 1, "units": "Week" },
"maxMessageSize": { "enabled": true, "mBytes": 2048 },
"sendEntireMessageSecurely": "LetUserChoose", "userEmailOption":
{ "allowToEnterToEmailAddress": true, "allowedDomains": {
"enabled": true, "list": [ "*.*" ] } }, "addressBookList": [
"user2<ivan@mail.com>", "User1<elver@mail.com>" ] } }, "links":
{ "self": "admin/v2/sites/df3be28b-f499-4b0a-9c53-
```


GET PowerShell Sample

```
####Added 2/10/2022 ###
###GET Drop Off Portal Settings###
Write-Output "GET Drop Off Portal Settings"
Write-Output "---------------------------"
#$siteID = "Enter site ID"
$DropOfflist = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/dropOffPortal" -Method 'GET' -Headers $authHeader
Write-Output $DropOfflist | ConvertTo-Json -Depth 25
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/dropOffPortal

PATCH Body Sample

```
### PATCH Drop Off Portal Settings###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/dropOffPortal/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "dropOffPortal",
    "attributes": {
      "enabled": true,
      "reservedPath": "/dropoff",
      "captcha": {
        "type": "reCAPTCHA",
        "value": {
          "siteKey": "6LeXY8odfasdfdsafdsafdsfsdfdsfdsfsdfdsfds-afar",
          "secretKey": "6Ldfasdfdsafdsafsdafdsafsdasfdsafdsfsd-afar"
        }
      },
      "linkExpiration": {
        "value": 1,
        "units": "Week"
      },
      "maxMessageSize": {
        "enabled": true,
        "mBytes": 2048
      },
      "sendEntireMessageSecurely": "LetUserChoose",
      "userEmailOption": {
        "allowToEnterToEmailAddress": true,
        "allowedDomains": {
          "enabled": true,
          "list": [
            "*.*"
          ]
        }
      },
      "addressBookList": ["user2<user2@mail.com>",
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type":
"dropOffPortal", "attributes": { "enabled": true, "reservedPath":
"/dropoff", "captcha": { "type": "reCAPTCHA", "value": { "siteKey":
"6LeXY8oUAAAAABIVq8RdygpeBeclHqrVBUd-afar", "secretKey":
"6LeXY8oUAAAAABIVq8RdygpeBeclHqrVBUd-afar" } }, "linkExpiration": {
"value": 1, "units": "Week" }, "maxMessageSize": { "enabled": true,
"mBytes": 2048 }, "sendEntireMessageSecurely": "LetUserChoose",
"userEmailOption": { "allowToEnterToEmailAddress": true,
"allowedDomains": { "enabled": true, "list": [ "*.*" ] } },
"addressBookList": [] } }, "links": { "self": "admin/v2/sites/0de7387f-
```


PATCH PowerShell Sample

```
Write-Output "PATCH Drop Off Portal Settings"
Write-Output "-----------------------------"
$update =
'{
  "data": {
    "type": "dropOffPortal",
    "attributes": {
      "enabled": true,
      "reservedPath": "/dropoff",
      "captcha": {
        "type": "reCAPTCHA",
        "value": {
          "siteKey": "6LeXY8odfasdfdsafdsafdsfsdfdsfdsfsdfdsfds-afar",
          "secretKey": "6Ldfasdfdsafdsafsdafdsafsdasfdsafdsfsd-afar"
```

Endpoint: /sites/{siteId}/privacyPolicy

Returns and updates the privacy policy configuration for specific site

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/privacyPolicy

GET Body Sample

```
### GET Privacy Policy  Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/privacyPolicy/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type":
"privacyPolicy", "attributes": { "type": "Mandatory", "values": {
"preventSftpsUntilAgreed": true, "impliedForNonSubjects": true },
"agreementPath": "", "agreementLabel": "", "effectiveDate": "Feb 11,
2022. 01:01:39 PM" } }, "links": { "self": "admin/v2/sites/0de7387f-1506-
427d-b997-e18bcdb8cbae/privacyPolicy" } }
```


GET PowerShell Sample

```
####Added 2/11/2022 ###
###GET Privacy Policy  Settings###
Write-Output "GET Privacy Policy  Settings"
Write-Output "----------------------------"
#$siteID = "Enter site ID"
$PPlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/privacyPolicy" -
Method 'GET' -Headers $authHeader
Write-Output $PPlist | ConvertTo-Json -Depth 25
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/privacyPolicy

PATCH Body Sample

```
### PATCH Privacy Policy  Settings###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/privacyPolicy/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "privacyPolicy",
    "attributes": {
      "type": "Mandatory",
      "values": {
        "preventSftpsUntilAgreed": false,
        "impliedForNonSubjects": false
      },
      "agreementPath": "",
      "agreementLabel": "",
      "effectiveDate": "Feb 11, 2020. 01:01:39 PM"
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type":
"privacyPolicy", "attributes": { "type": "Mandatory", "values": {
"preventSftpsUntilAgreed": false, "impliedForNonSubjects": false },
"agreementPath": "", "agreementLabel": "", "effectiveDate": "Feb 11,
2022. 01:01:39 PM" } }, "links": { "self": "/admin/v2/sites/0de7387f-
1506-427d-b997-e18bcdb8cbae/privacyPolicy" } }
```


PATCH PowerShell Sample

```
### PATCH Privacy Policy  Settings###
### User must obtain the SiteID from Get Sites
Write-Output "Privacy Policy  Settings"
Write-Output "------------------------------"
$update =
'{
  "data": {
    "type": "privacyPolicy",
    "attributes": {
      "type": "Mandatory",
      "values": {
        "preventSftpsUntilAgreed": true,
        "impliedForNonSubjects": true
      },
      "agreementPath": "",
      "agreementLabel": "",
      "effectiveDate": "Feb 11, 2020. 01:01:39 PM"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/privacyPolicy" -Method 'PATCH' -Headers $authHeader
-Body $update
```

Endpoint: /sites/{siteId}/termsOfService

Returns and updates the terms of service configuration for specific site

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/termsOfService

GET Body Sample

```
### GET Terms of Services Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/termsOfService/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type":
"termsOfService", "attributes": { "type": "Disabled", "agreementPath":
"", "agreementLabel": "", "effectiveDate": "Dec 16, 1950. 10:05:17 AM" }
}, "links": { "self": "admin/v2/sites/0de7387f-1506-427d-b997-
e18bcdb8cbae/termsOfService" } }
```


GET PowerShell Sample

```
###GET terms Of Service Settings###
Write-Output "GET GET terms Of Service Settings"
Write-Output "----------------------------"
#$siteID = "Enter site ID"
$TOSlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/termsOfService" -
Method 'GET' -Headers $authHeader
Write-Output $TOSlist | ConvertTo-Json -Depth 25
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/termsOfService

PATCH Body Sample

```
### PATCH Terms of Services Settings###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/termsOfService/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "termsOfService",
    "attributes": {
      "type": "Mandatory",
      "values": {
        "preventSftpsUntilAgreed": true
      },
      "agreementPath": "",
      "agreementLabel": "",
      "effectiveDate": "Dec 16, 2000. 10:05:17 AM"
    }
  }
}
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated Patch request(s).

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type":
"termsOfService", "attributes": { "type": "Mandatory", "values": {
"preventSftpsUntilAgreed": true }, "agreementPath": "", "agreementLabel":
"", "effectiveDate": "Feb 11, 2022. 01:01:53 PM" } }, "links": { "self":
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/termsOfService" } }
```


PATCH PowerShell Sample

```
####Added 2/11/2022
### PATCH terms Of Service Settings###
### User must obtain the SiteID from Get Sites
Write-Output "terms Of Service Settings"
Write-Output "-------------------------"
$update =
'{
  "data": {
    "type": "termsOfService",
    "attributes": {
      "type": "Mandatory",
      "values": {
        "preventSftpsUntilAgreed": true
      },
      "agreementPath": "",
      "agreementLabel": "",
      "effectiveDate": "Dec 16, 2000. 10:05:17 AM"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/termsOfService" -Method 'PATCH' -Headers
$authHeader -Body $update
```

Endpoint: /sites/{siteId}/gdpr

Returns and updates the GDPR configuration for specific profile

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/gdpr

GET Body Sample

```
### GET the GDRP Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/gdpr/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "gdpr",
"attributes": { "materialScope": "Unknown or undefined",
"territorialScope": { "type": "Unknown or undefined", "value": {
"showEUStatus": false, "allUsersToChangeEUSubject": false } },
"processingPrinciples": "Unknown or undefined", "lawfulnessOfProcessing":
"Unknown or undefined", "conditionsForConsent": "Unknown or undefined",
"ageRestrictions": "Unknown or undefined", "transparentInformation":
"Unknown or undefined", "directCollection": "Unknown or undefined",
"indirectCollection": "Unknown or undefined", "rightOfAccess": "Unknown
```


GET PowerShell Sample

```
###GET GDRP Settings###
Write-Output "GET GDRP Settings"
Write-Output "-----------------"
#$siteID = "Enter site ID"
$GDPRlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/gdpr" -Method
'GET' -Headers $authHeader
Write-Output $GDPRlist | ConvertTo-Json -Depth 25
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/gdpr

PATCH Body Sample

```
###PATCH the GDRP Settings###
PATCH  https://{{host}}/admin/v2/sites/{{Siteid}}/gdpr/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "gdpr",
    "attributes": {
      "materialScope": "In scope",
      "territorialScope": {
        "type": "In Union, all subjects in scope (3.1)",
        "value": {
          "showEUStatus": true,
          "allUsersToChangeEUSubject": true
        }
      },
      "processingPrinciples": "General guidance not yet met",
      "lawfulnessOfProcessing": "Data subject consent (6.1.a)",
      "conditionsForConsent": "Set via EFT's ToS or Privacy Policy",
```

PATCH Response Body Sample

The response will return the same response as the GET request, however, it will now include the updated PATCH request(s).


```
{ "data": { "id": "0de7387f-1506-427d-b997-e18bcdb8cbae", "type": "gdpr",
"attributes": { "materialScope": "In scope", "territorialScope": {
"type": "In Union, all subjects in scope (3.1)", "value": {
"showEUStatus": true, "allUsersToChangeEUSubject": true } },
"processingPrinciples": "General guidance not yet met",
"lawfulnessOfProcessing": "Data subject consent (6.1.a)",
"conditionsForConsent": "Set via EFT's ToS or Privacy Policy",
"ageRestrictions": "Enforced via EFT's ToS or Privacy Policy"
```


PATCH PowerShell Sample

```
### PATCH GDRP Settings###
### User must obtain the SiteID from Get Sites
Write-Output "PATCH GDRP Settings"
Write-Output "--------------------"
$update =
'{
  "data": {
    "type": "gdpr",
    "attributes": {
      "materialScope": "In scope",
      "territorialScope": {
        "type": "In Union, all subjects in scope (3.1)",
        "value": {
          "showEUStatus": true,
          "allUsersToChangeEUSubject": true
        }
      },
      "processingPrinciples": "General guidance not yet met",
      "lawfulnessOfProcessing": "Data subject consent (6.1.a)",
```

Endpoint: /sites/{siteId}/uploadForms

Returns and updates the upload forms configuration for specific profile

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/uploadForms

GET Body Sample

```
### GET the Upload Forms Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/uploadForms/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": [ { "type": "site", "id": "0de7387f-1506-427d-b997-
e18bcdb8cbae", "attributes": { "name": "MySite1" }, "links": { "self":
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae", "metrics":
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/metrics" } } ],
```


GET PowerShell Sample

```
###GET Upload Forms Settings###
Write-Output "GET Upload Forms Settings"
Write-Output "-----------------"
#$siteID = "Enter site ID"
$UpFormslist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/uploadForms"
-Method 'GET' -Headers $authHeader
Write-Output $UpFormslist | ConvertTo-Json -Depth 25
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/

POST Body Sample

```
###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/uploadForms/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "uploadFormName",
    "attributes": {
      "description": "Testing Forms from POST REST API",
      "displayName": "FORM_1",
      "displayInstruction": "Enter Text",
      "enabled": true,
      "showForEachFileUploaded": true,
      "userGroupId": "A0DB9377-92A3-4A38-8C0F-09F268D78FF1",
      "uploadFormElements": [
        {
          "name": "",
          "displayLabel": "FORM_1",
          "type": "string",
          "values": "domain.com",
          "required": true
        }
      ]
    }
  }
}
```

POST Response Body Sample


```
{"data":{"type":"uploadForm","id":"uploadFormName","attributes":{"id":"up
loadFormName","type":"uploadForm","attributes":{"description":"Testing
Forms from POST REST
API","displayName":"FORM_1","displayInstruction":"Enter
Text","enabled":true,"showForEachFileUploaded":true,"userGroupId":"a0db93
77-92a3-4a38-8c0f-
09f268d78ff1","uploadFormElements":[{"name":"","displayLabel":"FORM_1","t
ype":"String","values":"domain.com","required":true}]}}},"links":{"self":
"/admin/v2/sites/6203305a-d7c6-499e-a59b-
81500765f8f2/uploadForm/uploadFormName","userGroups":"/admin/v2/sites/620
```


POST PowerShell Sample

```
$update =
'{
  "data": {
    "id": "uploadFormName",
    "attributes": {
      "description": "Testing Forms from POST REST API",
      "displayName": "FORM_once",
      "displayInstruction": "Enter Text",
      "enabled": true,
      "showForEachFileUploaded": true,
      "userGroupId": "A0DB9377-92A3-4A38-8C0F-09F268D78FF1",
      "uploadFormElements": [
        {
          "name": "",
          "displayLabel": "FORM_once",
          "type": "string",
          "values": "domain.com",
          "required": true
        }
      ]
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$postUploadFormsReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/uploadForms" -Method 'POST' -Headers $authHeader -
Body $update
Write-Output $postUploadFormsReturn | ConvertTo-Json
```

Endpoint: /sites/{siteId}/uploadForms/{uploadFormName}

Returns site upload settings. Update site upload forms settings. Deletes upload form.

- GET
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/uploadForms/{uploadFormName}

GET Body Sample

```
### GET Specific Upload Forms Settings####
### Enter the form ID

@upLoadFormsID = {{formsList.response.body.$.data[0].id}}

GET
https://{{host}}/admin/v2/sites/{{Siteid}}/uploadForms/{{upLoadFormsID
}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{"data":{"id":"uploadFormName","type":"uploadForm","attributes":{"desc
ription":"Testing Forms from POST REST
API","displayName":"FORM_1","displayInstruction":"Enter
Text","enabled":true,"showForEachFileUploaded":true,"userGroupId":"a0d
b9377-92a3-4a38-8c0f-
09f268d78ff1","uploadFormElements":[{"name":"","displayLabel":"FORM_1"
,"type":"String","values":"domain.com","required":true}]}},"links":{"s
elf":"/admin/v2/sites/6203305a-d7c6-499e-a59b-
81500765f8f2/uploadForm/uploadFormName","userGroups":"/admin/v2/sites/
6203305a-d7c6-499e-a59b-81500765f8f2/userGroups"}}
```


GET PowerShell Sample

```
###GET Upload Forms Settings###
Write-Output "GET Upload Forms Settings"
Write-Output "-----------------"
#$siteID = "Enter site ID"
$UpFormslist = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/uploadForms" -Method 'GET' -Headers $authHeader
Write-Output $UpFormslist | ConvertTo-Json -Depth 25
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/uploadForms/{uploadFormName}

PATCH Body Sample

```
###
PATCH
https://{{host}}/admin/v2/sites/{{Siteid}}/uploadForms/{{upLoadFormsID
}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "uploadFormName",
    "type": "uploadForm",
    "attributes": {
      "description": "Testing Forms from POST REST API",
      "displayName": "FORM_1",
      "displayInstruction": "Enter Text",
      "enabled": true,
      "showForEachFileUploaded": false,
      "userGroupId": "a0db9377-92a3-4a38-8c0f-09f268d78ff1",
      "uploadFormElements": [
        {
          "name": "",
          "displayLabel": "FORM_1",
          "type": "String",
          "values": "domain.com",
          "required": true
        }
      ]
    }
  }
}
```

POST Response Body Sample


```
{"data":{"id":"uploadFormName","type":"uploadForm","attributes":{"desc
ription":"Testing Forms from POST REST
API","displayName":"FORM_1","displayInstruction":"Enter
Text","enabled":true,"showForEachFileUploaded":false,"userGroupId":"a0
db9377-92a3-4a38-8c0f-
09f268d78ff1","uploadFormElements":[{"name":"","displayLabel":"FORM_1"
,"type":"String","values":"domain.com","required":true}]}},"links":{"s
elf":"/admin/v2/sites/6203305a-d7c6-499e-a59b-
81500765f8f2/uploadForms/uploadFormName","userGroups":"/admin/v2/sites
/6203305a-d7c6-499e-a59b-81500765f8f2/userGroups"}}
```

PATCH PowerShell Sample

```
$update =
'{
  "data": {
    "id": "uploadFormName",
    "type": "uploadForm",
    "attributes": {
      "description": "Testing Forms from POST REST API",
      "displayName": "FORM_1",
      "displayInstruction": "Enter New Text",
      "enabled": true,
      "showForEachFileUploaded": false,
      "userGroupId": "a0db9377-92a3-4a38-8c0f-09f268d78ff1",
      "uploadFormElements": [
        {
          "name": "",
          "displayLabel": "FORM_1",
          "type": "String",
          "values": "domain.com",
          "required": true
        }
      ]
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchUploadFormsReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/uploadForms/$formsID" -Method 'PATCH' -Headers
$authHeader -Body $update
Write-Output $patchUploadFormsReturn | ConvertTo-Json
```

DELETE Body Sample

```
### GET Specific Upload Forms Settings####
### Enter the form ID

@upLoadFormsID = {{formsList.response.body.$.data[0].id}}

DELETE
https://{{host}}/admin/v2/sites/{{Siteid}}/uploadForms/{{upLoadFormsID
}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content
Date: Mon, 08 Aug 2022 20:43:09 GMT
Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate
Expires: -1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-
eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
$formsID = $uploadFList.data[0].id

$deleteUploadFList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/uploadForms/$formsID" -Method 'DELETE' -Headers
$authHeader
Write-Output $deleteUploadFList | ConvertTo-Json
```

Endpoint: /sites/{siteId}/userGroups

Returns the user groups for specific site

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/userGroups

GET Body Sample

```
### GET the User groups Settings####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/userGroups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": [ { "attributes": { "name": "All Users" }, "id": "A0DB9377-
92A3-4A38-8C0F-09F268D78FF1", "type": "userGroup" }, { "attributes": {
"name": "Administrators" }, "id": "07CACEB2-6698-4EF7-BAEB-F437FEC972A2",
"type": "userGroup" }, { "attributes": { "name": "Guests" }, "id":
```

GET PowerShell Sample

```
###GET User Groups###
Write-Output "GET User Groups"
Write-Output "----------------"
#$siteID = "Enter site ID"
$Uglist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/userGroups" -
Method 'GET' -Headers $authHeader
Write-Output $Uglist | ConvertTo-Json -Depth 25
```

Endpoint: /sites/{siteId}/outlookDeploymentScript

Returns the outlook deployment script.

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/outlookDeploymentScript

GET Body Sample

```
## GET outlook Deployment Script####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/outlookDeploymentScript
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
msiexec /lv installation.log /qn /i EFTOutlookAddinInstaller.msi
EFTHOST=http://172.31.223.227 EFTPORT=443 EFTAUTHTYPE=MANUAL
EFTUSERNAME=username EFTPASSWORD=test123!
INSTALLLOCATION="%userprofile%\AppData\Roaming\GlobalSCAPE\EFT Outlook
Add-in" FILESTORELOCATION="%userprofile%\AppData\Local\GlobalSCAPE\EFT
Outlook Add-in"
```

GET PowerShell Sample

```
###GET outlook Deployment Script###
Write-Output "GET outlook Deployment Script"
Write-Output "-----------------"
#$siteID = "Enter site ID"
$ODSlist = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/outlookDeploymentScript" -Method 'GET' -Headers
$authHeader
Write-Output $ODSlist | ConvertTo-Json -Depth 25
```

Endpoint: /sites/{siteId}/contentIntegrity

Returns and updates the content integrity settings for specific site.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/contentIntegrity

GET Body Sample

```
### GET a list of current content integrity profiles####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{ "data": [ { "id": "6f61c6c0-221e-4f01-94d0-46ba78ec0548", "type":
"contentIntegrity", "attributes": { "profileName": "TEST API" } }, {
"id": "03bebeda-1a89-40d2-a8c8-78ec078257db", "type": "contentIntegrity",
"attributes": { "profileName": "TEST API 2" } } ], "links": { "self":
"admin/v2/sites/0de7387f-1506-427d-b997-e18bcdb8cbae/contentIntegrity" }
```


GET PowerShell Sample

```
###GET list of Content Integrity Profiles###
Write-Output "GET list of Content Integrity Profiles"
Write-Output "-------------------------------------"
#$siteID = "Enter site ID"
$CIlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/contentIntegrity"
-Method 'GET' -Headers $authHeader
Write-Output $CIlist | ConvertTo-Json -Depth 25
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/contentIntegrity

POST Body Sample

```
### #POST content integrity profile ####
POST https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity/
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
  "data": {
    "type": "contentIntegrity",
    "attributes": {
      "profileName": "Profile_API_TEST5",
      "host": "192.168.100.82",
      "port": 1344,
      "path": "/reqmode",
      "mode": "REQMOD",
      "scanLimit": {
        "enabled": true,
        "bytes": 100000
      },
      "headerOverrides": {
        "httpHost": {
          "enabled": true,
          "value": "192.168.100.83"
        },
        "xClientIp": {
          "enabled": true,
          "value": "192.168.100.52"
        },
        "xServerIp": {
          "enabled": true,
          "value": "192.168.100.60"
        },
        "xSubscriberIp": {
          "enabled": true,
          "value": "192.168.100.70"
        },
        "xAuthenticatedUser": {
          "enabled": true,
```

POST Response Body Sample


```
{ "data": { "id": "53f00be5-9aa0-41ed-9fdf-ea99f6784238", "type":
"contentIntegrity", "attributes": { "profileName": "Profile_API_TEST",
"host": true, "port": 1344, "path": true, "mode": "REQMOD", "scanLimit":
{ "enabled": true, "bytes": 100000 }, "headerOverrides": { "httpHost": {
"enabled": true, "value": "192.168.100.83" }, "xClientIp": { "enabled":
true, "value": "192.168.100.52" }, "xServerIp": { "enabled": false,
```

POST PowerShell Sample

```
###POST Create New Content Integrity Profile###
Write-Output " Create New Content Integrity Profile"
Write-Output "-----------------------------------"
$update =
'{
  "data": {
    "type": "contentIntegrity",
    "attributes": {
      "profileName": "Profile_API_TEST6",
      "host": "192.168.100.82",
      "port": 1344,
      "path": "/reqmode",
      "mode": "REQMOD",
      "scanLimit": {
        "enabled": true,
        "bytes": 100000
      },
      "headerOverrides": {
        "httpHost": {
          "enabled": true
```

Endpoint: /sites/{siteId}/contentIntegrity/{profileId}

Returns, updates, and deletes content integrity profile settings.

- GET
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/contentIntegrity/{profileId}

GET Body Sample

```
### GET spacific content integrity profile settings####
###Pass the ID of the CIC profile###
@profileId = 53f00be5-9aa0-41ed-9fdf-ea99f6784238
GET
https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity/{{profileId}}
/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

Or

### GET spacific content integrity profile settings####
###Pass the ID of the CIC profile from another variable###
###@profileId = 53f00be5-9aa0-41ed-9fdf-ea99f6784238
```

GET Response Body Sample

```
{ "data": { "id": "53f00be5-9aa0-41ed-9fdf-ea99f6784238", "type":
"contentIntegrity", "attributes": { "profileName": "Profile_API_TEST",
"host": true, "port": 1344, "path": true, "mode": "REQMOD", "scanLimit":
{ "enabled": true, "bytes": 100000 }, "headerOverrides": { "httpHost": {
"enabled": true, "value": "192.168.100.83" }, "xClientIp": { "enabled":
true, "value": "192.168.100.52" }, "xServerIp": { "enabled": false,
"value": "" }, "xSubscriberIp": { "enabled": false, "value": "" },
"xAuthenticatedUser": { "enabled": false, "value": "" },
"xAuthenticatedGroups": { "enabled": false, "value": "" } },
"responseHandling": { "continueOnConnectivityError": "Continue",
"continueOnHttpError": "Continue", "continueOnIcapViolation": "Fail",
"continueOnIcapRedaction": "Continue", "customHeadersToAudit": {
"enabled": true, "headers": [] } } } }, "links": { "self":
"admin/v2/sites/0de7387f-1506-427d-b997-
```


GET PowerShell Sample

```
####Added 2/15/2022 ###
###GET specific Content Integrity Profile settings###
### User must obtain the Profile ID and manually enter it or by holding the
value on a variable ###
Write-Output "GET specific Content Integrity Profile settings"
Write-Output "-----------------------------------------------"
#$profileID = "53f00be5-9aa0-41ed-9fdf-ea99f6784238"
$SCIlist = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/contentIntegrity/$profileId" -Method 'GET' -Headers
$authHeader
Write-Output $SCIlist | ConvertTo-Json -Depth 35
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/contentIntegrity/{profileId}

PATCH Body Sample

```
### #PATCH content integrity profile ####
###Pass the ID of the CIC profile###
###@profileId = 53f00be5-9aa0-41ed-9fdf-ea99f6784238
PATCH
https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity/{{profileId}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
  "data": {
    "type": "contentIntegrity",
    "attributes": {
      "profileName": "Profile_API_TEST_PATCH",
      "host": true,
      "port": 1344,
      "path": true,
      "mode": "REQMOD",
      "scanLimit": {
        "enabled": true,
        "bytes": 100000
      },
      "headerOverrides": {
        "httpHost": {
          "enabled": true,
          "value": "192.168.100.00"
        },
        "xClientIp": {
          "enabled": true,
          "value": "192.168.100.00"
        },
        "xServerIp": {
          "enabled": false
```

PATCH Response Body Sample

```
{ "data": { "id": "d7c7c566-e2e1-4dd9-8332-9c2aa63f7bff", "type":
"contentIntegrity", "attributes": { "profileName":
"Profile_API_TEST_PATCH", "host": true, "port": 1344, "path": true,
"mode": "REQMOD", "scanLimit": { "enabled": true, "bytes": 100000 },
"headerOverrides": { "httpHost": { "enabled": true, "value":
"192.168.100.00" }, "xClientIp": { "enabled": true, "value":
"192.168.100.00" }, "xServerIp": { "enabled": false, "value": "" },
"xSubscriberIp": { "enabled": false, "value": "" }, "xAuthenticatedUser":
```

PATCH PowerShell Sample

```
### PATCH specific Content Integrity Profile settings###
### User must obtain the Profile ID and manually enter it or by holding the
value on a variable ###
Write-Output "PATCH specific Content Integrity Profile settings"
Write-Output "-------------------------------------------------"
$update =
'{
  "data": {
    "type": "contentIntegrity",
    "attributes": {
      "profileName": "Profile_API_TEST_PATCH",
      "host": true,
      "port": 1344,
      "path": true,
      "mode": "REQMOD",
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/contentIntegrity/{profileId}

DELETE Body Sample

```
###DELETE spacific content integrity profile settings####
###Pass the ID of the CIC profile###
###@profileId = 53f00be5-9aa0-41ed-9fdf-ea99f6784238
DELETE
https://{{host}}/admin/v2/sites/{{Siteid}}/contentIntegrity/{{profileId}}
/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
{ "data": [], "links": { "self": "/admin/v2/sites/0de7387f-1506-427d-
b997-e18bcdb8cbae/contentIntegrity" } }
```

DELETE PowerShell Sample

```
###DELETE specific content integrity profile settings####
###Pass the ID of the CIC profile###
###@profileId = 53f00be5-9aa0-41ed-9fdf-ea99f6784238
Write-Output "DELETE specific content integrity profile settings"
Write-Output "-------------------------------------------------"
#$profileID = "53f00be5-9aa0-41ed-9fdf-ea99f6784238"
$DCIClist = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/contentIntegrity/$profileId" -Method 'DELETE' -
Headers $authHeader
Write-Output $DCIClist | ConvertTo-Json -Depth 35
```

Endpoint: /sites/{siteId}/custom-commands

Note: Available as of EFT 8.1.0

This endpoint provides the ability to return a list of custom commands defined on an EFT site or create a new custom command.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/custom-commands

GET Body Sample

```
###
##Get Site Custom Commands
GET https://{{host}}/admin/v2//sites/{{siteId}}/custom-commands HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{ "data": [ { "id": "9a0c4aec-862e-4e72-aec4-9b1f04f00bb3", "type":
"customCommand", "attributes": { "name": "Command 1" }, "links": {
"self": "/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/custom-
commands/9a0c4aec-862e-4e72-aec4-9b1f04f00bb3" } }, { "id": "090dde3a-
c039-44ab-b03d-5cc994548ce7", "type": "customCommand", "attributes": {
"name": "Run to the Moon" }, "links": { "self":
"/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/custom-
```


GET PowerShell Sample

```
###
#Get Site Custom Commands
Write-Output "Get Site Custom Commands"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/custom-commands" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/custom-commands

POST Body Sample

```
## Create Custom Command on a specific EFT Site
POST https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data":{
        "id":"",
        "type": "customCommand",
            "attributes": {
                "enabled": true,
                "name": "Command 5",
                "description": "this is a test to run command 5",
                "executable": "c:\\windows\\system32\\cscript.exe
\"c:\\users\\administrator\\desktop\\server.vbs\"",
                "parameters": "",
                "redirectOutputToLog": true,
                "useProcessTimeOut": true,
                "processTimeOut": 30,
                "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log",
                "redirectOutputToClient": true,
                "useMinNumOfParams": false,
                "minNumOfParams": 1,
                "minNumOfParamsMsg": ""
            }
    }
}
###
```

POST Response Body Sample


```
{ "data": { "id": "f1d88549-e4aa-49da-b685-536fe0d93b62", "type":
"customCommand", "attributes": { "enabled": true, "name": "Command 5",
"description": "this is a test to run command 5", "executable":
"c:\\windows\\system32\\cscript.exe
\"c:\\users\\administrator\\desktop\\server.vbs\"", "parameters": "",
"redirectOutputToLog": true, "useProcessTimeOut": true, "processTimeOut":
30, "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log", "redirectOutputToClient": true,
"useMinNumOfParams": false, "minNumOfParams": 1, "minNumOfParamsMsg": ""
}, "relationships": { "executionPermissions": { "data": { "users": [],
"userGroups": [ { "type": "userGroup", "id": "a0db9377-92a3-4a38-8c0f-
09f268d78ff1", "meta": { "name": "All Users" } } ] } } }, "links": {
"self": "/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/custom-
```

POST PowerShell Sample

```
###
#POST new site Custom Command
Write-Output "POST Custom Command (New Custom Command)"
Write-Output "-----"
$update =
'{
    "data":{
        "id":"",
        "type": "customCommand",
            "attributes": {
                "enabled": true,
                "name": "Command 5",
                "description": "this is a test to run command 5",
                "executable": "c:\\windows\\system32\\cscript.exe
\"c:\\users\\administrator\\desktop\\server.vbs\"",
                "parameters": "",
                "redirectOutputToLog": true,
                "useProcessTimeOut": true,
                "processTimeOut": 30,
                "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log",
                "redirectOutputToClient": true,
                "useMinNumOfParams": false,
                "minNumOfParams": 1,
                "minNumOfParamsMsg": ""
            }
    }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-
```

Endpoint: /sites/{siteId}/custom-commands/{customCommandID}

Note: Available as of EFT 8.1.0

Returns a custom command defined on an EFT site and allows the ability to get, patch (update), and delete the custom command.

- GET
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/custom-commands/{customCommandID}

GET Body Sample

```
### Get Custom Commands for a Site ###
# @name customCommandList
GET https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@customCommandID = {{customCommandList.response.body.$.data[0].id}}

### Get specific Custom Command from a Site ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/custom-
commands/{{customCommandID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{ "data": { "id": "9a0c4aec-862e-4e72-aec4-9b1f04f00bb3", "type":
"customCommand", "attributes": { "enabled": true, "name": "Command 1",
"description": "this is a test to run command 1", "executable":
"c:\\windows\\system32\\cscript.exe
\"c:\\users\\administrator\\desktop\\server.vbs\"", "parameters": "",
"redirectOutputToLog": true, "useProcessTimeOut": true, "processTimeOut":
30, "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log", "redirectOutputToClient": true,
"useMinNumOfParams": false, "minNumOfParams": 1, "minNumOfParamsMsg": ""
}, "relationships": { "executionPermissions": { "data": { "users": [],
"userGroups": [ { "type": "userGroup", "id": "a0db9377-92a3-4a38-8c0f-
09f268d78ff1", "meta": { "name": "All Users" } } ] } } }, "links": {
```


GET PowerShell Sample

```
###
#Get Site Custom Commands
Write-Output "Get Site Custom Commands"
Write-Output "-----"
$commands = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-commands"
-Method 'GET' -Headers $authHeader
#Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($commands in $commands.id)
{
    Write-Output ("Custom Command found:  $($commands.id):
$($commands.attributes.name)")
}
$customCommandID = $commands.data[0].id

###
#Get Custom Command
Write-Output "Get Custom Commands for: "  $customCommandID
Write-Output "-----"
$commandList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-
commands/$customCommandID" -Method 'GET' -Headers $authHeader
Write-Output $commandList | ConvertTo-Json -Depth 10
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/custom-commands/{customCommandID}

PATCH Body Sample

```
### Get Custom Commands for a Site which is needed to patch a Custom
Commmand ###
# @name customCommandList
GET https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@customCommandID = {{customCommandList.response.body.$.data[0].id}}

###
#Path Custom Command on a specific EFT site
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/custom-
commands/{{customCommandID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data":{
        "id":"",
        "type": "customCommand",
            "attributes": {
                "enabled": true,
                "name": "Updated Custom Command Name",
                "description": "Updated Custom Command Description",
                "executable": "c:\\windows\\system32\\cscript.exe
\"c:\\users\\administrator\\desktop\\server.vbs\"",
                "parameters": "",
                "redirectOutputToLog": true,
                "useProcessTimeOut": false,
                "processTimeOut": 30,
                "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log",
                "redirectOutputToClient": true,
                "useMinNumOfParams": false,
                "minNumOfParams": 1,
                "minNumOfParamsMsg": ""
            }
    }
}
```

PATCH Response Body Sample

```
{ "data": { "id": "9a0c4aec-862e-4e72-aec4-9b1f04f00bb3", "type":
"customCommand", "attributes": { "enabled": true, "name": "Updated Custom
Command Name", "description": "Updated Custom Command Description",
"executable": "c:\\windows\\system32\\cscript.exe
\"c:\\users\\administrator\\desktop\\server.vbs\"", "parameters": "",
"redirectOutputToLog": true, "useProcessTimeOut": false,
"processTimeOut": 30, "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log", "redirectOutputToClient": true,
"useMinNumOfParams": false, "minNumOfParams": 1, "minNumOfParamsMsg": ""
}, "relationships": { "executionPermissions": { "data": { "users": [],
"userGroups": [ { "type": "userGroup", "id": "a0db9377-92a3-4a38-8c0f-
09f268d78ff1", "meta": { "name": "All Users" } } ] } } }, "links": {
```


PATCH PowerShell Sample

```
############################
#Patch a Custom Command
###
#Get Site Custom Commands
Write-Output "Get Site Custom Commands in order to Patch"
Write-Output "-----"
$commands = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-commands"
-Method 'GET' -Headers $authHeader
#Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($commands in $commands.id)
{
    Write-Output ("Custom Command found:  $($commands.id):
$($commands.attributes.name)")
}
$customCommandID = $commands.data[0].id

#PATCH Custom Command
Write-Output "Custom Command Patch"
Write-Output "Custom Command: $customCommandID"
Write-Output "-----"
$update =
'{
    "data":{
        "id":"",
        "type": "customCommand",
            "attributes": {
                "enabled": true,
                "name": "Updated Custom Command Name 2",
                "description": "Updated Custom Command Description 2",
                "executable": "c:\\windows\\system32\\cscript.exe
\"c:\\users\\administrator\\desktop\\server.vbs\"",
                "parameters": "",
                "redirectOutputToLog": true,
                "useProcessTimeOut": false,
                "processTimeOut": 30,
                "logFileName": "C:\\ProgramData\\Globalscape\\EFT
Server\\Logs\\cmdout.log",
                "redirectOutputToClient": true,
                "useMinNumOfParams": false,
                "minNumOfParams": 1,
                "minNumOfParamsMsg": ""
            }
    }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/custom-commands/{customCommandID}

DELETE Body Sample

```
##DELETE Custom Commands
### Get Custom Commands for a Site which is needed to delete a Custom
Commmand ###
# @name customCommandList
GET https://{{host}}/admin/v2/sites/{{Siteid}}/custom-commands HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@customCommandID = {{customCommandList.response.body.$.data[0].id}}
#

##Delete Request passing custom command id
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/custom-
commands/{{customCommandID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Fri, 15 Jul 2022 21:48:08 GMT Content-
Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-
Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
### DELETE CUSTOM COMMAND
#Get Site Custom Commands in order to get custom command id
Write-Output "Get Site Custom Commands in order to Delete"
Write-Output "-----"
$commands = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-commands"
-Method 'GET' -Headers $authHeader
#Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($commands in $commands.id)
{
    Write-Output ("Custom Command found:  $($commands.id):
$($commands.attributes.name)")
}
$customCommandID = $commands.data[0].id

Write-Output "Deleting Custom Command: "  $customCommandID
Write-Output "-----"
$commandList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/custom-
commands/$customCommandID" -Method 'DELETE' -Headers $authHeader
Write-Output $commandList | ConvertTo-Json -Depth 10
```

Endpoint: /sites/{siteId}/user-templates

Note: Available as of EFT 8.1.0

Returns a list of user templates defined on an EFT site and allows the ability to get and create templates.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/user-templates

GET Body Sample

```
### Get User Settings Template ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{ "data": [ { "attributes": { "as2": { "inbound": { "enabled": true },
"outbound": { "enabled": true } }, "changePassword": { "enabled":
"inherit", "value": { "changeAdminProvidedPasswordUponFirstUse":
"inherit", "passwordExpiration": { "enabled": true, "value": {
"maxAgeDays": 90, "emailUpon": true, "remindPrior": { "enabled": false,
"value": { "daysBefore": 5, "emailUser": true } } } } } },
"connectionTimeout": { "enabled": true, "value": { "maxSec": 600 } },
"connectionsFromSameIpLimit": { "enabled": false, "value": { "maxNumber":
0 } }, "downloadSizeLimit": { "enabled": false, "value": { "maxKBytes": 0
} }, "downloadsPerSessionLimit": { "enabled": false, "value": {
"maxNumber": 0 } }, "enabled": true, "ftp": { "enabled": true, "value": {
"enableFxp": "inherit", "enableNoop": "inherit", "enableComb": "yes",
"enableXcrc": "yes", "enableZlib": true, "banner": { "message": "Login
OK. Proceed.", "usage": "replaceDefault" } } }, "ftps": { "enabled": true
}, "hasHomeFolderAsRoot": true, "homeFolder": { "enabled": true, "value":
{ "path": "/" } }, "http": { "enableHttp": true, "enableHttps": true,
"enableWtc": true, "enableShareFolder": true, "enableSendMessage": true
}, "invalidLoginLimit": { "enabled": "inherit", "value": { "maxCount":
90, "periodMin": 5, "action": "lock", "actionDurationMin": 30 } },
"ipAccessLimit": { "enabled": false, "value": { "rules": [],
"defaultRule": "allowAccess" } }, "name": "Default Settings",
"passwordComplexity": { "enabled": "inherit", "value": { "minLength": 8,
```


GET PowerShell Sample

```
# get sites
Write-Output "Site"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites" -Method 'GET' -Headers
$authHeader
Write-Output $siteList | ConvertTo-Json
foreach ($site in $siteList.data)
{
    Write-Output ("Site  $($site.id): $($site.attributes.name)")
}

$siteID = $siteList.data[0].id

###
#Get Site User Settings Template
Write-Output "Get Site User Settings Template"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
##
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/user-templates

POST Body Sample

```
### POST User Settings Template (Create)###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data":{
        "type": "userTemplate",
        "attributes":{
            "name": "GSB Template 4",
            "accountEnabled": true,
            "homeFolder": {
                "enabled": false,
                "value": {
                    "path": ""
                }
            }
        },
        "passwordComplexity": {
          "enabled": "inherit",
          "value": {
            "minLength": 8,
            "characterCategories": {
              "enabled": true,
              "value": {
                "characterCount": 4,
                "upperCaseRequired": true,
                "lowerCaseRequired": true,
                "numericRequired": true,
                "nonAlphaNumericRequired": false,
                "non7bitAsciiRequired": false
              }
            },
            "usernameCharLimit": {
              "enabled": true,
              "value": {
                "minDisallowed": 3
              }
            }
          }
        },
        "sftp": {
          "enabled": true,
          "value": {
            "authenticationType": "password"
          }
        },
        "ssl": {
          "authenticationType": "password"
        }     }}
```

POST Response Body Sample


```
{ "data": { "attributes": { "as2": { "inbound": { "enabled": true },
"outbound": { "enabled": true } }, "changePassword": { "enabled":
"inherit", "value": { "changeAdminProvidedPasswordUponFirstUse":
"inherit", "passwordExpiration": { "enabled": true, "value": {
"maxAgeDays": 90, "emailUpon": true, "remindPrior": { "enabled": false,
"value": { "daysBefore": 5, "emailUser": true } } } } } },
"connectionTimeout": { "enabled": true, "value": { "maxSec": 600 } },
"connectionsFromSameIpLimit": { "enabled": false, "value": { "maxNumber":
0 } }, "downloadSizeLimit": { "enabled": false, "value": { "maxKBytes": 0
} }, "downloadsPerSessionLimit": { "enabled": false, "value": {
"maxNumber": 0 } }, "enabled": true, "ftp": { "enabled": true, "value": {
"enableFxp": "inherit", "enableNoop": "inherit", "enableComb": "yes",
"enableXcrc": "yes", "enableZlib": true, "banner": { "message": "Login
OK. Proceed.", "usage": "replaceDefault" } } }, "ftps": { "enabled": true
}, "hasHomeFolderAsRoot": true, "homeFolder": { "enabled": false,
"value": { "path": "/" } }, "http": { "enableHttp": true, "enableHttps":
true, "enableWtc": true, "enableShareFolder": true, "enableSendMessage":
true }, "invalidLoginLimit": { "enabled": "inherit", "value": {
"maxCount": 90, "periodMin": 5, "action": "lock", "actionDurationMin": 30
} }, "ipAccessLimit": { "enabled": false, "value": { "rules": [],
"defaultRule": "allowAccess" } }, "name": "GSB Template 4",
"passwordComplexity": { "enabled": "inherit", "value": { "minLength": 8,
"characterCategories": { "enabled": true, "value": { "characterCount": 4,
"upperCaseRequired": true, "lowerCaseRequired": true, "numericRequired":
true, "nonAlphaNumericRequired": false, "non7bitAsciiRequired": false }
}, "usernameCharLimit": { "enabled": true, "value": { "minDisallowed": 3
} }, "repeatingCharLimit": { "enabled": true, "value": { "minDisallowed":
3 } }, "forbiddenDictionary": { "enabled": true, "value": {
"dictionaryFilePath": "", "noBackwardsWord": false } } } },
"passwordHistory": { "enabled": "inherit", "value": { "historyDepth": 4 }
}, "sftp": { "enabled": true, "value": { "authenticationType": "password"
} }, "ssl": { "authenticationType": "password" },
"totalConnectionsLimit": { "enabled": false, "value": { "maxNumber": 0 }
```


POST PowerShell Sample

```
###
#POST Site User Settings Template (Create)
#POST new site Custom Command
Write-Output "POST User Settings Template (New User Settings Template)"
Write-Output "-----"
$update =
'{
    "data":{
        "type": "userTemplate",
        "attributes":{
            "name": "GSB Template 4",
            "accountEnabled": true,
            "homeFolder": {
                "enabled": false,
                "value": {
                    "path": ""
                }
            }
        },
        "passwordComplexity": {
          "enabled": "inherit",
          "value": {
            "minLength": 8,
            "characterCategories": {
              "enabled": true,
              "value": {
                "characterCount": 4,
                "upperCaseRequired": true,
                "lowerCaseRequired": true,
                "numericRequired": true,
                "nonAlphaNumericRequired": false,
                "non7bitAsciiRequired": false
              }
            },
            "usernameCharLimit": {
              "enabled": true,
              "value": {
                "minDisallowed": 3
              }
            }
          }
        },
        "sftp": {
          "enabled": true,
          "value": {
            "authenticationType": "password"
          }
        },
        "ssl": {
          "authenticationType": "password"
        }
      }

}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates" -Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/user-templates/{userTemplateid}

Note: Available as of EFT 8.1.0

Returns a user settings template defined on an EFT site and allows the ability to get, update, and delete the custom command.

- GET

- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/user-templates/{userTemplateid}

GET Body Sample

```
### Get User Settings Template ### Need to obtain templates first
# @name userTemplates
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@userTemplateid = {{userTemplates.response.body.$.data[3].id}}
#Update the array to obtain the desired user template


### GET User Template by Template ID ###
#
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-
templates/{{userTemplateid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": { "attributes": { "as2": { "inbound": { "enabled": true },
"outbound": { "enabled": true } }, "changePassword": { "enabled":
"inherit", "value": { "changeAdminProvidedPasswordUponFirstUse":
"inherit", "passwordExpiration": { "enabled": true, "value": {
"maxAgeDays": 90, "emailUpon": true, "remindPrior": { "enabled": false,
"value": { "daysBefore": 5, "emailUser": true } } } } } } },
"connectionTimeout": { "enabled": true, "value": { "maxSec": 600 } },
"connectionsFromSameIpLimit": { "enabled": false, "value": { "maxNumber":
0 } }, "downloadSizeLimit": { "enabled": false, "value": { "maxKBytes": 0
} }, "downloadsPerSessionLimit": { "enabled": false, "value": {
"maxNumber": 0 } }, "enabled": false, "ftp": { "enabled": true, "value":
{ "enableFxp": "inherit", "enableNoop": "inherit", "enableComb": "yes",
"enableXcrc": "yes", "enableZlib": true, "banner": { "message": "Login
OK. Proceed.", "usage": "replaceDefault" } } }, "ftps": { "enabled": true
}, "hasHomeFolderAsRoot": true, "homeFolder": { "enabled": true, "value":
{ "path": "/" } }, "http": { "enableHttp": true, "enableHttps": true,
"enableWtc": true, "enableShareFolder": true, "enableSendMessage": true
}, "invalidLoginLimit": { "enabled": "inherit", "value": { "maxCount":
90, "periodMin": 5, "action": "lock", "actionDurationMin": 30 } },
"ipAccessLimit": { "enabled": false, "value": { "rules": [],
"defaultRule": "allowAccess" } }, "name": "GSB Template 2",
"passwordComplexity": { "enabled": "inherit", "value": { "minLength": 8,
"characterCategories": { "enabled": true, "value": { "characterCount": 4,
"upperCaseRequired": true, "lowerCaseRequired": true, "numericRequired":
true, "nonAlphaNumericRequired": false, "non7bitAsciiRequired": false }
}, "usernameCharLimit": { "enabled": true, "value": { "minDisallowed": 3
} }, "repeatingCharLimit": { "enabled": true, "value": { "minDisallowed":
3 } }, "forbiddenDictionary": { "enabled": true, "value": {
"dictionaryFilePath": "", "noBackwardsWord": false } } } },
"passwordHistory": { "enabled": "inherit", "value": { "historyDepth": 4 }
}, "sftp": { "enabled": true, "value": { "authenticationType": "password"
} }, "ssl": { "authenticationType": "password" },
"totalConnectionsLimit": { "enabled": false, "value": { "maxNumber": 0 }
```


GET PowerShell Sample

```
#######################################
#GET Specific User Settings Template

###
#Get Specific User Settings Templates
Write-Output "Get Specific User Settings Template"
Write-Output "-----"
$userTemplates = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($userTemplates in $userTemplates.id)
{
    Write-Output ("User Template found:  $($userTemplates.id):
$($userTemplates.attributes.name)")
}
$userTemplateID = $userTemplates.data[3].id

###
#Get Specific User Template
Write-Output "Get User Template for: "  $userTemplateID " with name: "
$userTemplate.data.attributes.name
Write-Output "-----"
$userTemplate = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates/$userTemplateID" -Method 'GET' -Headers $authHeader
Write-Output $userTemplate | ConvertTo-Json -Depth 10
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/user-templates/{userTemplateid}

PATCH Body Sample

```
### Get User Settings Template ### Need to obtain templates first
# @name userTemplates
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@userTemplateid = {{userTemplates.response.body.$.data[3].id}}
#Update the array to obtain the desired user template


### PATCH User Template by Template ID
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/user-
templates/{{userTemplateid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data": {
        "type": "userTemplate",
        "attributes": {
            "enabled": false,
            "homeFolder": {
                "enabled": true,
                "value": {
                    "path": ""
                }
            }
        }
    }
}
```

PATCH Response Body Sample

```
{ "data": { "attributes": { "as2": { "inbound": { "enabled": true },
"outbound": { "enabled": true } }, "changePassword": { "enabled":
"inherit", "value": { "changeAdminProvidedPasswordUponFirstUse":
"inherit", "passwordExpiration": { "enabled": true, "value": {
"maxAgeDays": 90, "emailUpon": true, "remindPrior": { "enabled": false,
"value": { "daysBefore": 5, "emailUser": true } } } } } } },
"connectionTimeout": { "enabled": true, "value": { "maxSec": 600 } },
"connectionsFromSameIpLimit": { "enabled": false, "value": { "maxNumber":
0 } }, "downloadSizeLimit": { "enabled": false, "value": { "maxKBytes": 0
} }, "downloadsPerSessionLimit": { "enabled": false, "value": {
"maxNumber": 0 } }, "enabled": false, "ftp": { "enabled": true, "value":
{ "enableFxp": "inherit", "enableNoop": "inherit", "enableComb": "yes",
"enableXcrc": "yes", "enableZlib": true, "banner": { "message": "Login
OK. Proceed.", "usage": "replaceDefault" } } }, "ftps": { "enabled": true
}, "hasHomeFolderAsRoot": true, "homeFolder": { "enabled": true, "value":
{ "path": "/" } }, "http": { "enableHttp": true, "enableHttps": true,
"enableWtc": true, "enableShareFolder": true, "enableSendMessage": true
}, "invalidLoginLimit": { "enabled": "inherit", "value": { "maxCount":
90, "periodMin": 5, "action": "lock", "actionDurationMin": 30 } },
"ipAccessLimit": { "enabled": false, "value": { "rules": [],
"defaultRule": "allowAccess" } }, "name": "GSB Template 2",
"passwordComplexity": { "enabled": "inherit", "value": { "minLength": 8,
"characterCategories": { "enabled": true, "value": { "characterCount": 4,
"upperCaseRequired": true, "lowerCaseRequired": true, "numericRequired":
true, "nonAlphaNumericRequired": false, "non7bitAsciiRequired": false }
}, "usernameCharLimit": { "enabled": true, "value": { "minDisallowed": 3
} }, "repeatingCharLimit": { "enabled": true, "value": { "minDisallowed":
3 } }, "forbiddenDictionary": { "enabled": true, "value": {
"dictionaryFilePath": "", "noBackwardsWord": false } } } },
"passwordHistory": { "enabled": "inherit", "value": { "historyDepth": 4 }
}, "sftp": { "enabled": true, "value": { "authenticationType": "password"
} }, "ssl": { "authenticationType": "password" },
"totalConnectionsLimit": { "enabled": false, "value": { "maxNumber": 0 }
```


PATCH PowerShell Sample

```
#####################################################
##PATCH (Update) specific User Settings Template
###
#Get Specific User Settings Templates
Write-Output "Get Specific User Settings Template"
Write-Output "-----"
$userTemplates = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($userTemplates in $userTemplates.id)
{
    Write-Output ("User Template found:  $($userTemplates.id):
$($userTemplates.attributes.name)")
}
$userTemplateID = $userTemplates.data[3].id

###
#Get Specific User Template
Write-Output "Get User Template for: "  $userTemplateID " with name: "
$userTemplate.data.attributes.name
Write-Output "-----"
$userTemplate = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates/$userTemplateID" -Method 'GET' -Headers $authHeader
Write-Output $userTemplate | ConvertTo-Json -Depth 10


###
##Patch Specific User Settings Template
Write-Output "User Settings Template Patch (update)"
Write-Output "-----"
$update =
'{
    "data":{
        "type": "userTemplate",
          "attributes": {
            "enabled": false,
            "homeFolder": {
                "enabled": true,
                "value": {
                    "path": ""
                }
            }
        }
    }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates/$userTemplateID" -Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/user-templates/{userTemplateid}

DELETE Body Sample

```
###
#Delete Specific User Settings Template
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/user-
templates/{{userTemplateid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
#
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Thu, 21 Jul 2022 13:38:16 GMT Content-
Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-
Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
############################################################
#Delete User Settings Template

#Get Specific User Settings Templates
Write-Output "Get Specific User Settings Template"
Write-Output "-----"
$userTemplates = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
foreach ($userTemplates in $userTemplates.id)
{
    Write-Output ("User Template found:  $($userTemplates.id):
$($userTemplates.attributes.name)")
}
$userTemplateID = $userTemplates.data[3].id

###
#Get Specific User Template
Write-Output "Get User Template for: "  $userTemplateID " with name: "
$userTemplate.data.attributes.name
Write-Output "-----"
$userTemplate = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates/$userTemplateID" -Method 'GET' -Headers $authHeader
Write-Output $userTemplate | ConvertTo-Json -Depth 10

#Delete Request
Write-Output "Deleting User Settings Template: "  $userTemplateID
Write-Output "-----"
$commandList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
templates/$userTemplateID" -Method 'DELETE' -Headers $authHeader
Write-Output $commandList | ConvertTo-Json -Depth 10
```

Endpoint: /sites/{siteId}/user-groups

Note: Available as of EFT 8.1.0

Provides the ability to return a .list of user groups for a specific EFT site or create a new permission group.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups

GET Body Sample

```
### Get List of all User's Permissions Groups for the Site####
#
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{ "data": [ { "type": "userGroup", "id": "a0db9377-92a3-4a38-8c0f-
09f268d78ff1", "attributes": { "name": "All Users" }, "relationships": {
"users": { "data": [ { "type": "user", "id": "b90be871-86ff-4060-b3cc-
007903dff7f7", "meta": { "name": "Ivan" } }, { "type": "user", "id":
"953bcb67-fa8c-44e2-a056-ecfb5080d13c", "meta": { "name": "TestUser" } }
] } }, "links": { "self": "/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-
01a10524c048/user-groups/a0db9377-92a3-4a38-8c0f-09f268d78ff1" } }, {
"type": "userGroup", "id": "07caceb2-6698-4ef7-baeb-f437fec972a2",
"attributes": { "name": "Administrators" }, "relationships": { "users": {
"data": [] } }, "links": { "self": "/admin/v2/sites/c7d3ecfe-a100-4bcd-
b830-01a10524c048/user-groups/07caceb2-6698-4ef7-baeb-f437fec972a2" } },
{ "type": "userGroup", "id": "b8448b77-01d8-47d5-8ee7-9f407c95e39f",
"attributes": { "name": "Guests" }, "relationships": { "users": { "data":
```


GET PowerShell Sample

```
# Get sites
Write-Output "Site"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites" -Method 'GET' -Headers
$authHeader
Write-Output $siteList | ConvertTo-Json
foreach ($site in $siteList.data)
{
    Write-Output ("Site  $($site.id): $($site.attributes.name)")
}

$siteID = $siteList.data[0].id
##########
#Get User Permission Groups
Write-Output "Get User Permission Groups"
Write-Output "-----"
$userGroups = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups" -
Method 'GET' -Headers $authHeader
Write-Output $userGroups | ConvertTo-Json -Depth 10
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups

POST Body Sample

```
### Create User Permission Group ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data": {
        "type": "userGroup",
        "attributes": {
            "name": "QA_API_User_Group_TEST"
        }
    }
}
```

POST Response Body Sample

```
{ "data": { "type": "userGroup", "id": "1ba8c63f-6e37-4783-b556-
be5bf831dc6c", "attributes": { "name": "QA_API_User_Group_TEST" },
"relationships": { "users": { "data": [] } }, "links": { "self":
"/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/user-
```

POST PowerShell Sample

```
#POST New Permission Group
Write-Output "POST User Permissions Group (New Permission Group)"
Write-Output "-----"
$update =
'{
  "data": {
        "type": "userGroup",
        "attributes": {
            "name": "QA_API_User_Group_TEST"
        }
    }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups"
-Method 'POST' -Headers $authHeader -Body $update
```

Endpoint: /sites/{siteId}/user-groups/{groupid}

Note: Available as of EFT 8.1.0

Provides the ability to return a user group's details, update a permission group name or delete a user group.

- GET
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups/{groupid}

GET Body Sample

```
### Get List of all User's Permissions Groups for the Site####
# @name UGlist
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@groupid = {{UGlist.response.body.$.data[3].id}}


### GET Details for specific User Permission Group####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups/{{groupid}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "type": "userGroup", "id": "7386d09b-ac9d-42c8-a7dd-
8ffb840d58e3", "attributes": { "name": "QA_API_User_Group_TEST" },
"relationships": { "users": { "data": [] } }, "links": { "self":
"/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/user-
groups/7386d09b-ac9d-42c8-a7dd-8ffb840d58e3" } } }
```

GET PowerShell Sample

```
##########
#Get User Permission Groups
$userGroups = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups" -
Method 'GET' -Headers $authHeader
foreach ($userGroups in $userGroups.id)
{
    Write-Output ("User Permission Group found:  $($userGroups.id):
$($userGroups.attributes.name)")
}
$userGroupID = $userGroups.data[3].id


#Get Specific User Permission Group
Write-Output "Get Specific User Permission Group"
Write-Output "-----"
$userGroup = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID" -Method 'GET' -Headers $authHeader
Write-Output $userGroup | ConvertTo-Json -Depth 10
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups/{groupid}

PATCH Body Sample

```
### GET Details for specific User Permission Group####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups/{{groupid}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###

#### Update Name for Specific User Permissions Group
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}//user-groups/{{groupid}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
   "data": {
    "type": "userGroup",
    "attributes": {
      "name": "QA_API_User_Group_TEST2"
    }
```

PATCH Response Body Sample

```
{ "data": { "type": "userGroup", "id": "7386d09b-ac9d-42c8-a7dd-
8ffb840d58e3", "attributes": { "name": "QA_API_User_Group_TEST2" },
"relationships": { "users": { "data": [] } }, "links": { "self":
"/admin/v2/sites/c7d3ecfe-a100-4bcd-b830-01a10524c048/user-
groups/7386d09b-ac9d-42c8-a7dd-8ffb840d58e3" } } }
```

PATCH PowerShell Sample

```
#Get Specific User Permission Group
Write-Output "Get Specific User Permission Group"
Write-Output "-----"
$userGroup = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID" -Method 'GET' -Headers $authHeader
Write-Output $userGroup | ConvertTo-Json -Depth 10

###
##Patch Specific User Permissions Group
Write-Output "User Permission Group Patch (update)"
Write-Output "-----"
$update =
'{
   "data": {
    "type": "userGroup",
    "attributes": {
      "name": "QA_API_User_Group_TEST2"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID" -Method 'PATCH' -Headers $authHeader -Body $update
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups/{groupid}

DELETE Body Sample

```
### Delete Specific User Permission Group ###
Delete https://{{host}}/admin/v2/sites/{{Siteid}}//user-
groups/{{groupid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Fri, 22 Jul 2022 22:40:06 GMT Content-
Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-
Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
#Get Specific User Permission Group
Write-Output "Get Specific User Permission Group"
Write-Output "-----"
$userGroup = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID" -Method 'GET' -Headers $authHeader
Write-Output $userGroup | ConvertTo-Json -Depth 10

###
#DELETE Specific User Permission Group
Write-Output "Delete Specific User Permission Group"
Write-Output "-----"
$commandList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID" -Method 'DELETE' -Headers $authHeader
Write-Output $commandList | ConvertTo-Json -Depth 10
```

Endpoint: /sites/{siteId}/user-groups/{groupid}/relationships/users

Note: Available as of EFT 8.1.0

Provides the ability to return a user group's details, update a permission group name or delete a user group.

- POST
- DELETE

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups/{groupid}/relationships/users

POST Body Sample

```
###Get Users
# @name user
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@userid = {{user.response.body.$.data[3].id}}
#Store a user into a variable in order to add to a group later

###
### Get List of all User's Permissions Groups for the Site####
# @name UGlist
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@groupid = {{UGlist.response.body.$.data[3].id}}
#Store a user group in order to add a user to this group later

### Add User(s) to specific Permission Group ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/user-
groups/{{groupid}}/relationships/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": [
    {
      "type": "user",
      "id": "{{userid}}"
    }
   ]
}
```

POST Response Body Sample

```
{ "data": [ { "type": "user", "id": "b90be871-86ff-4060-b3cc-
007903dff7f7", "meta": { "name": "Ivan" } } ] }
```

POST PowerShell Sample

```
##
#Get User Permission Groups
$userGroups = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups" -
Method 'GET' -Headers $authHeader
foreach ($userGroups in $userGroups.id)
{
Write-Output ("User Permission Group found:  $($userGroups.id):
$($userGroups.attributes.name)")
}
$userGroupID = $userGroups.data[3].id

###
#POST Selected User in Selected User Permission Group
Write-Output "POST (Add) User to Selected User Permissions Group"
Write-Output "-----"
$update =
'{
  "data": [
    {
      "type": "user",
      "id": "b90be871-86ff-4060-b3cc-007903dff7f7"
    }
  ]
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID/relationships/users" -Method 'POST' -Headers $authHeader -
Body $update
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/user-groups/{groupid}/relationships/users

DELETE Body Sample

```
###Get Users
# @name user
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@userid = {{user.response.body.$.data[3].id}}
#Store a user into a variable in order to add to a group later

###
### Get List of all User's Permissions Groups for the Site####
# @name UGlist
GET https://{{host}}/admin/v2/sites/{{Siteid}}/user-groups HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@groupid = {{UGlist.response.body.$.data[3].id}}
#Store a user group in order to add a user to this group later


### Delete User(s) from specific Permission Group ###
Delete https://{{host}}/admin/v2/sites/{{Siteid}}/user-
groups/{{groupid}}/relationships/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": [
    {
      "type": "user",
      "id": "{{userid}}"
    }
  ]
}
```

DELETE Response Body Sample

```
HTTP/1.1 200 OK Date: Sat, 23 Jul 2022 01:47:11 GMT Content-Type:
application/vnd.api+json Content-Length: 11 Cache-Control: no-cache, no-
store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-
Protection: 1; mode=block Content-Security-Policy: default-src 'self'
'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer {
"data": [] }
```

DELETE PowerShell Sample

```
##
#Get User Permission Groups
$userGroups = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-groups" -
Method 'GET' -Headers $authHeader
foreach ($userGroups in $userGroups.id)
{
      Write-Output ("User Permission Group found:  $($userGroups.id):
$($userGroups.attributes.name)")
}
$userGroupID = $userGroups.data[3].id

#Delete User from User Permission Group
Write-Output "Deleting User from User Permission Group: "
Write-Output "-----"
$update =
'{
  "data": [
    {
      "type": "user",
      "id": "b90be871-86ff-4060-b3cc-007903dff7f7"
    }
  ]
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$commandList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/user-
groups/$userGroupID/relationships/users" -Method 'DELETE' -Headers $authHeader
-Body $update
```

Endpoint: /sites/{siteId}/ram/agents

Note: Available as of EFT 8.1.0

Returns a list of remote agents from a specified site.

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ram/agents

GET Body Sample

```
### GET Remote Agents
GET  https://{{host}}/admin/v2/sites/{{Siteid}}/ram/agents HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
##
```

GET Response Body Sample

```
{ "data": [ { "id": "4dfd3f28-6ba9-4e19-ae7b-4d3b0b4314f6", "type":
"remote-agent", "attributes": { "name": "ag_IV-2019A", "clid": "00000000-
0000-0000-0000-000000000000", "state": "PendingJoin", "pausing": false,
"resuming": false, "netBios": "IV-2019A", "domain": "", "winOEM": "x64
(AMD or Intel)", "ips": [ "fe80::904:aa5a:7256:ca57 (Ethernet)",
"10.91.160.123 (Ethernet)", "ff01::1 (Ethernet)", "ff02::1 (Ethernet)",
"ff02::c (Ethernet)", "ff02::fb (Ethernet)", "ff02::1:3 (Ethernet)",
"ff02::1:ff56:ca57 (Ethernet)", "224.0.0.1 (Ethernet)", "224.0.0.251
(Ethernet)", "224.0.0.252 (Ethernet)", "239.255.255.250 (Ethernet)", "::1
(Loopback Pseudo-Interface 1)", "127.0.0.1 (Loopback Pseudo-Interface
1)", "ff02::c (Loopback Pseudo-Interface 1)", "239.255.255.250 (Loopback
Pseudo-Interface 1)" ], "macAddresses": [ "0-15-5d-64-e-2c" ],
"lastUpdate": 0, "version": "8.1.0.6", "lastKnownIP": "10.91.160.123",
"nextUpdate": 0, "approvedTime": 0, "secret":
"7102da9c0219696b82679072b9c2f6e6d46fc0da9aa58d3fc1aa2e94f7858cde",
"peakVersion": "8.1.0.6" }, "links": { "self": "/admin/v2/sites/4ebb829f-
f84c-4355-8d55-d43a2852ca12/ram/agents/4dfd3f28-6ba9-4e19-ae7b-
4d3b0b4314f6" } }, { "id": "6ad61dcb-fabe-4627-aebe-065cfe4eadd0",
"type": "remote-agent", "attributes": { "name": "ag_IV-2019C", "clid":
"00000000-0000-0000-0000-000000000000", "state": "PendingJoin",
"pausing": false, "resuming": false, "netBios": "IV-2019C", "domain": "",
"winOEM": "x64 (AMD or Intel)", "ips": [ "fe80::2d7d:3dd6:4ff0:9bba
(Ethernet)", "10.91.160.130 (Ethernet)", "ff01::1 (Ethernet)", "ff02::1
(Ethernet)", "ff02::c (Ethernet)", "ff02::fb (Ethernet)", "ff02::1:3
(Ethernet)", "ff02::1:fff0:9bba (Ethernet)", "224.0.0.1 (Ethernet)",
"224.0.0.251 (Ethernet)", "224.0.0.252 (Ethernet)", "239.255.255.250
(Ethernet)", "::1 (Loopback Pseudo-Interface 1)", "127.0.0.1 (Loopback
Pseudo-Interface 1)", "ff02::c (Loopback Pseudo-Interface 1)",
"239.255.255.250 (Loopback Pseudo-Interface 1)" ], "macAddresses": [ "0-
15-5d-64-e-2e" ], "lastUpdate": 0, "version": "8.1.0.6", "lastKnownIP":
```


GET PowerShell Sample

```
# Get sites
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites" -Method 'GET' -Headers
$authHeader
$siteID = $siteList.data[0].id

###GET Remote Agents
Write-Output "Remote Agents"
Write-Output "----"
$ramAgentList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ram/agents"
-Method 'GET' -Headers $authHeader
Write-Output $ramAgentList | ConvertTo-Json
foreach ($ramAgentList in $ramAgentList.data)
{
    Write-Output ("Remote Agent  $($ramAgentList.id):
$($ramAgentList.attributes.name)")
}
```

Endpoint: /sites/{siteId}/ram/agents/{remoteAgentID}

Note: Available as of EFT 8.1.0

Returns a remote agent's settings from a specified site.

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ram/agents/{remoteAgentID}

GET Body Sample

```
### GET Remote Agents
# @name RAMList
GET  https://{{host}}/admin/v2/sites/{{Siteid}}/ram/agents HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
##
###
@remoteAgentID = {{RAMList.response.body.$.data[0].id}}

##
#Get Specific RAM Agent ID
GET
https://{{host}}/admin/v2/sites/{{Siteid}}/ram/agents/{{remoteAgentID}}
HTTP/1.1
```

GET Response Body Sample


```
{ "data": { "id": "4dfd3f28-6ba9-4e19-ae7b-4d3b0b4314f6", "type":
"remote-agent", "attributes": { "name": "ag_IV-2019A", "clid": "00000000-
0000-0000-0000-000000000000", "state": "PendingJoin", "pausing": false,
"resuming": false, "netBios": "IV-2019A", "domain": "", "winOEM": "x64
(AMD or Intel)", "ips": [ "fe80::904:aa5a:7256:ca57 (Ethernet)",
"10.91.160.123 (Ethernet)", "ff01::1 (Ethernet)", "ff02::1 (Ethernet)",
"ff02::c (Ethernet)", "ff02::fb (Ethernet)", "ff02::1:3 (Ethernet)",
"ff02::1:ff56:ca57 (Ethernet)", "224.0.0.1 (Ethernet)", "224.0.0.251
(Ethernet)", "224.0.0.252 (Ethernet)", "239.255.255.250 (Ethernet)", "::1
(Loopback Pseudo-Interface 1)", "127.0.0.1 (Loopback Pseudo-Interface
1)", "ff02::c (Loopback Pseudo-Interface 1)", "239.255.255.250 (Loopback
Pseudo-Interface 1)" ], "macAddresses": [ "0-15-5d-64-e-2c" ],
"lastUpdate": 0, "version": "8.1.0.6", "lastKnownIP": "10.91.160.123",
"nextUpdate": 0, "approvedTime": 0, "secret":
"7102da9c0219696b82679072b9c2f6e6d46fc0da9aa58d3fc1aa2e94f7858cde",
"peakVersion": "8.1.0.6" }, "links": { "self": "/admin/v2/sites/4ebb829f
```


GET PowerShell Sample

```
###GET Remote Agents
Write-Output "Remote Agents"
Write-Output "----"
$ramAgentList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/ram/agents"
-Method 'GET' -Headers $authHeader
$ramAgentID = $ramAgentList.data[0].id

###GET Remote Agent Settings
Write-Output "GET Specific Remote Agent Settings: " $ramAgentID
Write-Output "----"
$ramAgent = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/agents/$ramAgentID" -Method 'GET' -Headers
$authHeader
Write-Output $ramAgent | ConvertTo-Json
```

Endpoint: /sites/{siteId}/ram/agents/templates

Note: Available as of EFT 8.1.0

Returns a remote agent template list from a specified site or allows the creation of a template on a specific EFT site.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ram/templates

GET Body Sample

```
########################
#RAM TEMPLATES
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{ "data": [ { "id": "04cd2f6f-dea6-4674-bcde-3c7fe5a800a1", "type":
"remote-agents-template", "attributes": { "name": "RAM Template1",
"updateInterval": "EveryFiveMinutes", "eventRuleIds": [ null, "d352632d-
5f3f-49bf-99af-849f7453dd0a" ], "autoEnroll": false, "autoEnrollDate":
1659757989, "homeFolder": "/Usr/Agents/%AgentNetBIOSName%/",
"updateFailure": "Stop_Disable_Unenroll", "enableIPAccess": false,
"ipAccess": { "masks": [ { "ipMask": "0.0.0.0", "reason": "",
"matchAction": "Deny", "timeStamp": 0, "autobanEntry": true } ],
"autoban": [], "defaultAction": "Allow" } }, "links": { "self":
"/admin/v2/sites/4ebb829f-f84c-4355-8d55-
d43a2852ca12/ram/templates/04cd2f6f-dea6-4674-bcde-3c7fe5a800a1" } }, {
"id": "b672dec5-567e-4baa-bc3f-5be948802b42", "type": "remote-agents-
template", "attributes": { "name": "RAM Template 2", "updateInterval":
```

GET PowerShell Sample

```
###############
##GET Remote Agent Templates
Write-Output "Remote Agent Templates"
Write-Output "----"
$ramTemplateList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates" -Method 'GET' -Headers $authHeader
Write-Output $ramTemplateList | ConvertTo-Json -Depth 10
foreach ($ramTemplateList in $ramTemplateList.data)
{
    Write-Output ("Remote Agent Template  $($ramTemplateList.id):
$($ramTemplateList.attributes.name)")
}
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/ram/templates

POST Body Sample

```
### Add New RAM Template ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
      "name": "NewRAMTemplateName",
      "updateInterval": "EveryFiveMinutes",
      "eventRuleIds": [
        "d352632d-5f3f-49bf-99af-849f7453dd0a"
      ],
      "autoEnroll": true,
      "autoEnrollDate": 0,
      "homeFolder": "/Usr/Agents/%AgentNetBIOSName%/",
      "updateFailure": "Stop_Disable_Unenroll",
      "enableIPAccess": true,
      "ipAccess": {
        "masks": [
          {
            "ipMask": "0.0.0.0",
            "reason": "",
            "matchAction": "Deny",
            "timeStamp": 0,
            "autobanEntry": true
          }
        ],
        "defaultAction": "Allow"
      }
    }
  }
}
```

POST Response Body Sample


```
{ "data": { "id": "b3ed1f50-ce61-479f-ba48-094cee3c13fd", "type":
"remote-agents-template", "attributes": { "name": "NewRAMTemplateName",
"updateInterval": "EveryFiveMinutes", "eventRuleIds": [ null, "d352632d-
5f3f-49bf-99af-849f7453dd0a" ], "autoEnroll": true, "autoEnrollDate": 0,
"homeFolder": "/Usr/Agents/%AgentNetBIOSName%/", "updateFailure":
"Stop_Disable_Unenroll", "enableIPAccess": true, "ipAccess": { "masks": [
{ "ipMask": "0.0.0.0", "reason": "", "matchAction": "Deny", "timeStamp":
0, "autobanEntry": false } ], "autoban": [], "defaultAction": "Allow" }
}, "links": { "self": "/admin/v2/sites/4ebb829f-f84c-4355-8d55-
d43a2852ca12/ram/templates/b3ed1f50-ce61-479f-ba48-094cee3c13fd" } } }
```

POST PowerShell Sample

```
#######
###
#POST New RAM Template
Write-Output "POST RAM Template"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes": {
      "name": "NewRAMTemplateName",
      "updateInterval": "EveryFiveMinutes",
      "eventRuleIds": [
        "d352632d-5f3f-49bf-99af-849f7453dd0a"
      ],
      "autoEnroll": true,
      "autoEnrollDate": 0,
      "homeFolder": "/Usr/Agents/%AgentNetBIOSName%/",
      "updateFailure": "Stop_Disable_Unenroll",
      "enableIPAccess": true,
      "ipAccess": {
        "masks": [
          {
            "ipMask": "0.0.0.0",
            "reason": "",
            "matchAction": "Deny",
            "timeStamp": 0,
            "autobanEntry": true
          }
        ],
        "defaultAction": "Allow"
      }
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates" -Method 'POST' -Headers $authHeader
-Body $update
```

Endpoint: /sites/{siteId}/ram/agents/templates/{remoteAgentsTemplateID}

Note: Available as of EFT 8.1.0

Returns a remote agent settings template from a specified site, update/patch a remote agent settings template, or allows the deletion of a remote agent settings template on a specific EFT site.

- GET
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/ram/templates/{remoteAgentsTemplateID}

GET Body Sample

```
############################
#GET RAM Template by ID
#RAM TEMPLATES
# @name RAMTemplates
GET https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
@ramTemplateID = {{RAMTemplates.response.body.$.data[0].id}}


###
#GET Template by Template ID
GET
https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates/{{ramTemplateID}
} HTTP/1.1
```

GET Response Body Sample


```
{ "data": { "id": "04cd2f6f-dea6-4674-bcde-3c7fe5a800a1", "type":
"remote-agents-template", "attributes": { "name": "RAM Template1",
"updateInterval": "EveryFiveMinutes", "eventRuleIds": [], "autoEnroll":
false, "autoEnrollDate": 1659757989, "homeFolder":
"/Usr/Agents/%AgentNetBIOSName%/", "updateFailure":
"Stop_Disable_Unenroll", "enableIPAccess": false, "ipAccess": { "masks":
[ { "ipMask": "0.0.0.0", "reason": "", "matchAction": "Deny",
"timeStamp": 0, "autobanEntry": false } ], "autoban": [],
"defaultAction": "Allow" } }, "links": { "self":
"/admin/v2/sites/4ebb829f-f84c-4355-8d55-
```


GET PowerShell Sample

```
###############
##GET Remote Agent Templates
$ramTemplateList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates" -Method 'GET' -Headers $authHeader
$ramTemplateID = $ramTemplateList.data[0].id

####
#GET Remote Agent Template by ID
Write-Output "Remote Agent Template by ID: " $ramTemplateID
Write-Output "----"
$ramTemplate = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates/$ramTemplateID" -Method 'GET' -
Headers $authHeader
Write-Output $ramTemplate | ConvertTo-Json -Depth 10
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/ram/templates/{remoteAgentsTemplateID}

PATCH Body Sample

```
####
#PATCH Template by Template ID
PATCH
https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates/{{ramTemplateID}
} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
        "ipAccess": {
        "masks": [
          {
            "ipMask": "0.0.0.0",
            "reason": "",
            "matchAction": "Deny",
            "timeStamp": 0,
            "autobanEntry": false
          }
        ],
        "defaultAction": "Allow"
      }
    }
  }
`
```

PATCH Response Body Sample

```
{ "data": { "id": "04cd2f6f-dea6-4674-bcde-3c7fe5a800a1", "type":
"remote-agents-template", "attributes": { "name": "RAM Template1",
"updateInterval": "EveryFiveMinutes", "eventRuleIds": [], "autoEnroll":
false, "autoEnrollDate": 1659757989, "homeFolder":
"/Usr/Agents/%AgentNetBIOSName%/", "updateFailure":
"Stop_Disable_Unenroll", "enableIPAccess": false, "ipAccess": { "masks":
[ { "ipMask": "0.0.0.0", "reason": "", "matchAction": "Deny",
"timeStamp": 0, "autobanEntry": false } ], "autoban": [],
"defaultAction": "Allow" } }, "links": { "self":
```

PATCH PowerShell Sample

```
##########
##GET Remote Agent Template ID
$ramTemplateList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates" -Method 'GET' -Headers $authHeader
$ramTemplateID = $ramTemplateList.data[0].id

###
##Patch Remote Agent Template by ID
Write-Output "Remote Agent Template Patch (update)"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes": {
        "ipAccess": {
        "masks": [
          {
            "ipMask": "1.1.1.1",
            "reason": "",
            "matchAction": "Deny",
            "timeStamp": 0,
            "autobanEntry": false
          }
        ],
        "defaultAction": "Allow"
      }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates/$ramTemplateID" -Method 'PATCH' -
Headers $authHeader -Body $update
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/ram/templates/{remoteAgentsTemplateID}

DELETE Body Sample

```
####
#DELETE Remote Agent Template
#Template must not have existing associated Remote Agents
DELETE
https://{{host}}/admin/v2/sites/{{Siteid}}/ram/templates/{{ramTemplateID}
} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Sun, 24 Jul 2022 02:05:46 GMT Content-
Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-
Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
###################################
##########
##GET Remote Agent Template ID
$ramTemplateList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates" -Method 'GET' -Headers $authHeader
$ramTemplateID = $ramTemplateList.data[1].id

####
#DELETE Remote Agent Template by ID
$ramTemplateList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/ram/templates/$ramTemplateID" -Method 'DELETE' -
Headers $authHeader
```

Endpoint:/sites/{siteId}/awe-tasks

Note: Available as of EFT 8.1.0

(GET) Returns advanced workflow task list from specified site and (POST) creates advanced workflow task for specified site

- GET
- POST

Method & URL

GET https://{{host}}/admin/v2/sites/{{SiteId}}/awe-tasks

GET Body Sample

```
### GET AWE TASKS ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{"data":[{"id":"0f340ef3-3628-5844-bb6b-
c659252b6b44","type":"aweTask","attributes":{"name":"Sample - Date Format
Functions","created":"2022-08-
01","description":""},"relationships":{"aweFolder":{"data":{"id":"0000000
0-0000-0000-0000-
000000000000","name":"<root>"}}},"links":{"self":"/admin/v2/sites/b65892e
9-399d-4447-a3b1-477c08f0abca/awe-tasks/0f340ef3-3628-5844-bb6b-
c659252b6b44"}},{"id":"92ac1ba6-5fcc-5b85-b5da-
e1b3c4d4a300","type":"aweTask","attributes":{"name":"Sample - Environment
Variables","created":"2022-08-
01","description":""},"relationships":{"aweFolder":{"data":{"id":"0000000
0-0000-0000-0000-
000000000000","name":"<root>"}}},"links":{"self":"/admin/v2/sites/b65892e
9-399d-4447-a3b1-477c08f0abca/awe-tasks/92ac1ba6-5fcc-5b85-b5da-
e1b3c4d4a300"}},{"id":"432c99b4-fcf3-5472-981d-
416946a9b95a","type":"aweTask","attributes":{"name":"Sample - Excel
Actions","created":"2022-08-
01","description":""},"relationships":{"aweFolder":{"data":{"id":"0000000
0-0000-0000-0000-
000000000000","name":"<root>"}}},"links":{"self":"/admin/v2/sites/b65892e
```


GET PowerShell Sample

```
# get awe-tasks
Write-Output "AWE-TASKS"
Write-Output "-----"
$aweList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks" -
Method 'GET' -Headers $authHeader
Write-Output $aweList | ConvertTo-Json
foreach ($awetask in $aweList.data)
{
    Write-Output ("Task ID $($aweTask.id): Name ->
$($aweTask.attributes.name)")
}
```

POST https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks

POST Body Sample

```
POST https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "aweTask",
    "attributes": {

"code":"PEFNVEFTSz4NCjxBTVRBU0tIRUFEPg0KICAgIDxUQVNLSU5GTyBUQVNLVkVSU0lPT
j0iMTAuNy4xMDAuMSIgLz4NCjwvQU1UQVNLSEVBRD4NCg0KPEFNRlVOQ1RJT04gTkFNRT0iTW
FpbiIgQUNDRVNTPSJwcml2YXRlIiBSRVRVUk5UWVBFPSJ2YXJpYWJsZSI+DQo8IS0tIC0tLS0
tLS0tLS0gLS0+DQo8IS0tIEdFTkVSQUwgVEFTSyBOT1RFUzogIFRoaXMgdGFzayB3aWxsIG91
dHB1dCBhbGwgc3VwcG9ydGVkIGVudmlyb25tZW50IHZhcmlhYmxlcyB0byBhIHRleHQgZmlsZ
S4gWW91IGNhbiB1c2UgdGhlc2UgdmFyaWFibGVzIGluc2lkZSBvZiBBV0UgdGFza3Mgd2hlcm
UgbmVlZGVkLg0KDQpUaGUgZmlsZSB3aWxsIGJlIGNhbGVsZCAiZW52aXJvbm1lbnQgdmFyaWF
ibGVzIiBhbmQgcGxhY2VkIG9uIHRoZSByb290IG9mIHlvdXIgZHJpdmUgKHVzdWFsbHkgYzpc
KS4gLS0+DQo8IS0tIC0tLS0tLS0tLS0gLS0+DQo8QU1FTlZWQVJTIEFDVElWRVRZPSJsaXN0I
iBSRVNVTFREQVRBU0VUPSJFbnZybXRWYXJEYXRhc2V0IiBUWVBFPSJtYWNoaW5lIiAvPg0KIC
AgICA8QU1GSUxFU1lTVEVNIEFDVElWRVRZPSJ3cml0ZV9maWxlIiBGSUxFPSIlU3lzdGVtRHJ
```

POST Response Body Sample

```
{"data":{"id":"8405b064-aa9a-46b8-b0b5-
4c60eb3d3e09","type":"aweTask","attributes":{"name":"MyNewAWEScript","cre
ated":"2022-08-01","description":"Hello,
world!","useTimeout":true,"timeout":10,"logLevel":"Verbose","logDirectory
":"","retainSuccessfulLogs":false,"retainFailedLogs":true,"code":"PEFNVEF
TSz4NCjxBTVRBU0tIRUFEPg0KICAgIDxUQVNLSU5GTyBUQVNLVkVSU0lPTj0iMTAuNy4xMDAu
MSIgLz4NCjwvQU1UQVNLSEVBRD4NCg0KPEFNRlVOQ1RJT04gTkFNRT0iTWFpbiIgQUNDRVNTP
SJwcml2YXRlIiBSRVRVUk5UWVBFPSJ2YXJpYWJsZSI+DQo8IS0tIC0tLS0tLS0tLS0gLS0+DQ
o8IS0tIEdFTkVSQUwgVEFTSyBOT1RFUzogIFRoaXMgdGFzayB3aWxsIG91dHB1dCBhbGwgc3V
wcG9ydGVkIGVudmlyb25tZW50IHZhcmlhYmxlcyB0byBhIHRleHQgZmlsZS4gWW91IGNhbiB1
c2UgdGhlc2UgdmFyaWFibGVzIGluc2lkZSBvZiBBV0UgdGFza3Mgd2hlcmUgbmVlZGVkLg0KD
QpUaGUgZmlsZSB3aWxsIGJlIGNhbGVsZCAiZW52aXJvbm1lbnQgdmFyaWFibGVzIiBhbmQgcG
xhY2VkIG9uIHRoZSByb290IG9mIHlvdXIgZHJpdmUgKHVzdWFsbHkgYzpcKS4gLS0+DQo8IS0
tIC0tLS0tLS0tLS0gLS0+DQo8QU1FTlZWQVJTIEFDVElWRVRZPSJsaXN0IiBSRVNVTFREQVRB
U0VUPSJFbnZybXRWYXJEYXRhc2V0IiBUWVBFPSJtYWNoaW5lIiAvPg0KICAgICA8QU1GSUxFU
1lTVEVNIEFDVElWRVRZPSJ3cml0ZV9maWxlIiBGSUxFPSIlU3lzdGVtRHJ
```

POST PowerShell Sample

```
##POST SITE AWE TASKS
Write-Output "Site AWE TASK POST"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "aweTask",
    "attributes": {

"code":"PEFNVEFTSz4NCjxBTVRBU0tIRUFEPg0KICAgIDxUQVNLSU5GTyBUQVNLVkVSU0lPTj0iMT
AuNy4xMDAuMSIgLz4NCjwvQU1UQVNLSEVBRD4NCg0KPEFNRlVOQ1RJT04gTkFNRT0iTWFpbiIgQUND
RVNTPSJwcml2YXRlIiBSRVRVUk5UWVBFPSJ2YXJpYWJsZSI+DQo8IS0tIC0tLS0tLS0tLS0gLS0+DQ
o8IS0tIEdFTkVSQUwgVEFTSyBOT1RFUzogIFRoaXMgdGFzayB3aWxsIG91dHB1dCBhbGwgc3VwcG9y
dGVkIGVudmlyb25tZW50IHZhcmlhYmxlcyBObyBhIHRleHQgZmlsZS4gWW91IGNhbiB1c2UgdGhlc2
UgdmFyaWFibGVzIGluc2lkZSBvZiBBV0UgdGFza3Mgd2hlcmUgbmVlZGVkLg0KDQpUaGUgZmlsZSB3
aWxsIGJlIGNhbGVsZCAiZW52aXJvbm1lbnQgdmFyaWFibGVzIiBhbmQgcGxhY2VkIG9uIHRoZSByb2
90IG9mIHlvdXIgZHJpdmUgKHVzdWFsbHkgYzpcKS4gLS0+DQo8IS0tIC0tLS0tLS0tLS0gLS0+DQo8
QU1FTlZWQVJTIEFDVElWSVRZPSJsaXN0IiBSRVNVTFREQVRBU0VUPSJFbnZybXRWYXJEYXRhc2V0Ii
BUWVBFPSJtYWNoaW5lIiAvPg0KICAgICA8QU1GSUxFU1lTVEVNIEFDVElWSVRZPSJ3cml0ZV9maWxl
IiBGSUxFPSIlU3lzdGVtRHJpdmUlXGVudmlyb25tZW50X3ZhcmlhYmxlcyI+RW52aXJvbm1lbnQgdm
FyaWFibGVzIGZvciBtYWNoaW5lIChzeXN0ZW0pOg0KDQo8L0FNRklMRVNZU1RFTT4NCiAgICAgPC9BTUxPT1A+DQo8QU1FTlZWQVJTIEFDVElW
SVRZPSJsaXN0IiBSRVNVTFREQVRBU0VUPSJFbnZybXRWYXJEYXRhc2V0IiBUWVBFPSJ1c2VyIiAvPg
0KICAgICA8QU1GSUxFU1lTVEVNIEFDVElWSVRZPSJ3cml0ZV9maWxlIiBGSUxFPSIlU3lzdGVtRHJp
dmUlXGVudmlyb25tZW50X3ZhcmlhYmxlcyI+DQpFbnZpcm9ubWVudCB2YXJpYWJsZXMgZm9yIFVzZX
```

Endpoint:/sites/{siteId}/awe-tasks/{aweTaskID}

Note: Available as of EFT 8.1.0

(GET) Returns advanced workflow task from specified site, (PATCH) Updates advanced workflow task settings, and (DELETE) Delete advanced workflow task

- GET
- PATCH
- DELETE

Method & URL

GET https://{{host}}/admin/v2/sites/{{SiteId}}/awe-tasks/{aweTaskID}

GET Body Sample

```
### GET A SPECIFIC AWE TASK
@aweID = {{aweList.response.body.$.data[0].id}}
GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks/{{aweID}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{"data":{"id":"0f340ef3-3628-5844-bb6b-
c659252b6b44","type":"aweTask","attributes":{"name":"Sample - Date Format
Functions","created":"2022-08-
01","description":"","useTimeout":true,"timeout":120,"logLevel":"None","l
ogDirectory":"C:\\ProgramData\\Globalscape\\EFT
Server\\AWE\\Temp\\","retainSuccessfulLogs":true,"retainFailedLogs":true,
"code":"PEFNVEFTSz4NCjxBTVRBU0tIRUFEPg0KICAgIDxUQVNLSU5GTyBUQVNLVkVSU0lPT
j0iMTAuNy4xMDAuMSIgLz4NCjwvQU1UQVNLSEVBRD4NCg0KPEFNRlVOQ1RJT04gTkFNRT0iTW
FpbiIgQUNDRVNTPSJwcml2YXRlIiBSRVRVUk5UWVBFPSJ2YXJpYWJsZSI+DQo8IS0tIC0tLS0
tLS0tLS0gLS0+DQo8IS0tIEdFTkVSQUwgVEFTSyBOT1RFUzogIFRoaXMgdGFzayByZXR1cm5z
IHRoZSBjdXJyZW50IHN5c3RlbSB0aW1lIGluIGEgbnVtYmVyIG9mIGRpZmZlcmVudCBmb3JtY
XRzIHVzaW5nIHRoZSBGb3JtYXQoKSBmdW5jdGlvbi4gLS0+DQo8IS0tIC0tLS0tLS0tLS0gLS
```


GET PowerShell Sample

```
# get awe-tasks
Write-Output "AWE-TASKS"
Write-Output "-----"
$aweList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks" -
Method 'GET' -Headers $authHeader
Write-Output $aweList | ConvertTo-Json
foreach ($awetask in $aweList.data)
{
    Write-Output ("Task ID $($aweTask.id): Name ->
$($aweTask.attributes.name)")
}

$aweID = $aweList.data[0].id
$awsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks/$aweID"
-Method 'GET' -Headers $authHeader
Write-Output $awsList | ConvertTo-Json
```

PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks/{{aweID}}

PATCH Body Sample

```
### UPDATE A SPECIFIC AWE TASK (this is using the environment var code)
### for your site you may have to adjust the index number
@aweID = {{aweList.response.body.$.data[14].id}}
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks/{{aweID}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
  "data": {
    "type": "aweTask",
    "attributes": {
      "logDirectory": "C\\temp\\"
    }
  }
}
```

PATCH Response Body Sample


```
{"data":{"id":"8405b064-aa9a-46b8-b0b5-
4c60eb3d3e09","type":"aweTask","attributes":{"name":"MyNewAWEScript","cre
ated":"2022-08-01","description":"Hello,
world!","useTimeout":true,"timeout":10,"logLevel":"Verbose","logDirectory
":"C\\temp\\","retainSuccessfulLogs":false,"retainFailedLogs":true,"code"
:"PEFNVEFTSz4NCjxBTVRBU0tIRUFEPg0KICAgIDxUQVNLSU5GTyBUQVNLVkVSU0lPTj0iMTA
uNy4xMDAuMSIgLz4NCjwvQU1UQVNLSEVBRD4NCg0KPEFNRlVOQ1RJT04gTkFNRT0iTWFpbiIg
QUNDRVNTPSJwcml2YXRlIiBSRVRVUk5UWVBFPSJ2YXJpYWJsZSI+DQo8IS0tIC0tLS0tLS0tL
S0gLS0+DQo8IS0tIEdFTkVSQUwgVEFTSyBOT1RFUzogIFRoaXMgdGFzayB3aWxsIG91dHB1dC
BhbGwgc3VwcG9ydGVkIGVudmlyb25tZW50IHZhcmlhYmxlcyB0byBhIHRleHQgZmlsZS4gWW9
1IGNhbiB1c2UgdGhlc2UgdmFyaWFibGVzIGluc2lkZSBvZiBBV0UgdGFza3Mgd2hlcmUgbmVl
ZGVkLg0KDQpUaGUgZmlsZSB3aWxsIGJlIGNhbGVsZCAiZW52aXJvbm1lbnQgdmFyaWFibGVzI
```


PATCH PowerShell Sample

```
##PATCH SITE AWE TASKS
Write-Output "Site specific AWE TASK PATCH"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "aweTask",
    "attributes": {
      "description": "Well Hello",
      "useTimeout": true,
      "timeout": 10,
      "logLevel": "Verbose",
      "retainSuccessfulLogs": true,
      "retainFailedLogs": true
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchAWETASKReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-
tasks/$aweID" -Method 'PATCH' -Headers $authHeader -Body $update
```

DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks/{{aweID}}

DELETE Body Sample

```
### DELETE A SPECIFIC AWE TASK
@aweID = {{aweList.response.body.$.data[0].id}}

DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks/{{aweID}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content

Date: Mon, 01 Aug 2022 21:16:00 GMT

Content-Length: 0

Cache-Control: no-cache, no-store, must-revalidate

Expires: -1

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;
```

DELETE PowerShell Sample

```
$aweID = $aweList.data[0].id
$awsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks/$aweID"
-Method 'DELETE' -Headers $authHeader
Write-Output $awsList | ConvertTo-Json
```

Endpoint:/sites/{siteId}/awe-tasks-folders

Note: Available as of EFT 8.1.0

(GET) Returns advanced workflow folder list from specified site and (POST) create advanced workflow folder for specified site

- GET
- POST

Method & URL

GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-task-folders

GET Body Sample

```
### GET ALL AWE TASK FOLDERS ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{"data":[{"id":"00000000-0000-0000-0000-
000000000000","type":"aweFolder","attributes":{"name":"<root>","tasks":[{
"id":"92ac1ba6-5fcc-5b85-b5da-e1b3c4d4a300","name":"Sample - Environment
Variables","created":"2022-08-01","description":""},{"id":"432c99b4-fcf3-
5472-981d-416946a9b95a","name":"Sample - Excel Actions","created":"2022-
08-01","description":""},{"id":"df5f43bb-1f34-57be-9e59-
75bd272ba408","name":"Sample - Expectations","created":"2022-08-
01","description":""},{"id":"cf774000-2d0a-5962-a060-
111aa4d94d1c","name":"Sample - File Date Operations","created":"2022-08-
01","description":""},{"id":"40536ad8-327e-53d6-8566-
0d7722156b42","name":"Sample - FTP Actions","created":"2022-08-
01","description":""},{"id":"a6a79232-f9e5-5a14-b944-
```


GET PowerShell Sample

```
####Added 2/01/2020
### Returns all site auto ban list###
Write-Output "AWE Task Folders"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-
folders" -Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

POST https://{{host}}/admin/v2/sites/{{Siteid}}/awe-task-folders

POST Body Sample

```
### create a folder named AWE_Folder_Three
###

###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "aweTaskFolder",
    "attributes": {
      "name": "AWE_Folder_Three"
    }
  }
}
###
```

POST Response Body Sample

```
{"data":{"id":"dc70ad42-47ad-4239-a81a-
fe9d650820aa","type":"aweFolder","attributes":{"name":"AWE_Folder_Three",
"tasks":[]},"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-
477c08f0abca/awe-tasks-folders/dc70ad42-47ad-4239-a81a-
fe9d650820aa"}},"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-
477c08f0abca/awe-tasks-folders"}}
```


POST PowerShell Sample

```
####Added 2/01/2020
### Returns all site auto ban list###
Write-Output "AWE Task Folders"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-
folders" -Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json

##POST SITE AWE TASKS FOLDERS
Write-Output "Site AWE TASK FOLDER POST"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "aweTaskFolder",
    "attributes": {
      "name": "AWE_Folder_FIVE-O"
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$postAWETASKReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-
tasks-folders" -Method 'POST' -Headers $authHeader -Body $update
Write-Output $postAWETASKReturn | ConvertTo-Json
```

Endpoint:/sites/{sitetId}/awe-tasks-folders/{aweTaskFolderID}

Note: Available as of EFT 8.1.0

(GET) Returns advanced workflow folder from specified site, (PATCH) Updates advanced workflow folder settings, and (DELETE) Delete advanced workflow folder.

- GET
- PATCH
- DELETE

Method & URL

GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders/{{AWEId}}

GET Body Sample

```
### GET A SPECIFIC AWE TASK FOLDERS ###
@AWEId = 859dc605-0600-42ab-a1fa-f23f5a19e8cd
GET https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders/{{AWEId}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{"data":{"id":"859dc605-0600-42ab-a1fa-
f23f5a19e8cd","type":"aweFolder","attributes":{"name":"AWE _
Folder_One","tasks":[]},"links":{"self":"/admin/v2/sites/b65892e9-399d-
4447-a3b1-477c08f0abca/awe-tasks-folders/859dc605-0600-42ab-a1fa-
f23f5a19e8cd"}},"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-
477c08f0abca/awe-tasks-folders"}}
```


GET PowerShell Sample

```powershell
####Added 2/01/2020
### Returns awe folder information###
Write-Output "AWE Task Folders"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-
folders" -Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json

$aweID = $siteList.data[1].id
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-tasks-
folders/$aweID" -Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders/{{AWEId}}

PATCH Body Sample

```
@AWEId = dc70ad42-47ad-4239-a81a-fe9d650820aa
### PATCH AWE TASK FOLDERS ###
PATCH  https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-
folders/{{AWEId}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "id": "dc70ad42-47ad-4239-a81a-fe9d650820aa",
    "attributes": {
      "name": "NewFirstFolder"
    },
    "type": "aweTaskFolder"
  }
}
```

PATCH Response Body Sample


```
{"data":{"id":"dc70ad42-47ad-4239-a81a-
fe9d650820aa","type":"aweFolder","attributes":{"name":"NewFirstFolder","t
asks":[{"id":"432c99b4-fcf3-5472-981d-416946a9b95a","name":"Sample -
Excel Actions","created":"2022-08-01","description":"My
Description"},{"id":"40536ad8-327e-53d6-8566-0d7722156b42","name":"Sample
- FTP Actions","created":"2022-08-
01","description":""}]},"links":{"self":"/admin/v2/sites/b65892e9-399d-
4447-a3b1-477c08f0abca/awe-tasks-folders/dc70ad42-47ad-4239-a81a-
fe9d650820aa"}},"links":{"self":"/admin/v2/sites/b65892e9-399d-4447-a3b1-
```


PATCH PowerShell Sample

```
$folderID = $aweFolderList.data[1].id

##POST SITE AWE TASKS FOLDERS
Write-Output "Site AWE TASK FOLDER PATCH"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "aweTaskFolder",
    "attributes": {
      "name": "TEST FOLDER TWO"
    }
  }
}'

$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchAWETASKReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-
tasks-folders/$folderID" -Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $patchAWETASKReturn | ConvertTo-Json
```

DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/awe-tasks-folders/{{AWEId}}

NOTE: The folder should be emptied before it is deleted else the EFT will return a HTTP 500 Server error.

DELETE Body Sample

```
### AWEId will be the id of a folder to be deleted.
@AWEId = e1d62bf1-8bdd-4e82-8efd-395467069306
### DELETE AWE TASK FOLDERS ###
DELETE  https://{{host}}/admin/v2/sites/{{Siteid}}/awe-task-
folders/{{AWEId}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content
Date: Tue, 02 Aug 2022 17:47:50 GMT
Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate
Expires: -1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
$folderID = $aweFolderList.data[1].id

$deleteAWETASKReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/awe-
tasks-folders/$folderID" -Method 'DELETE' -Headers $authHeader
Write-Output $deleteAWETASKReturn | ConvertTo-Json
```

Endpoint: /sites/{siteId}/connection-profiles

Note: Available as of EFT 8.1.0

(GET) Returns connection profiles list from the specified site, (POST) create a connection profile for a site.

- GET
- POST

Method & URL

```
GET https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles
```

GET Body Sample

```
### GET a list of current connection profiles####
GET https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
HTTP/1.1 200 OK Date: Thu, 04 Aug 2022 14:17:24 GMT Location:
/admin/v2/sites/76882fc7-3f55-4040-ae5f-2e645c12647b/connection-profiles
Content-Type: application/vnd.api+json Content-Length: 1383 Cache-Control:
no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options:
nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src
'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer {
"data": [ { "id": "c9ea36ec-8a9e-440f-8c21-920eb3927732", "type":
"connectionProfile", "attributes": { "type": "Protocol", "name": "POST
REQUEST Create connection Profile", "description": "Connection Profile
Details", "connectionSettings": { "protocol": "FTPSAuthTLS", "user": "AFAR",
"password": "UpKUJq1sD4Yfb1Hz8ZFiRw==", "autoLogin": true, "testPath":
```


GET PowerShell Sample

```
####################################
###GET list of Connection Profiles###
Write-Output "GET list of Connection Profiles"
Write-Output "------------------------------"
#$siteID = "Enter site ID"
$CPlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/connection-
Profiles" -Method 'GET' -Headers $authHeader
Write-Output $CPlist | ConvertTo-Json -Depth 25

$profileId = $CPList.data[0].id
```

Method & URL

```
POST https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles
```

POST Body Sample

```
### Create a Connection Profile ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles/ HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
 "data":{
  "type":"connectionProfile",
  "attributes":{
   "name":"POST REQUEST Create connection Profile",
   "description":"Connection Profile Details",
   "testPath":"\test",
   "connectionSettings":{
    "protocol":"FTPSAuthTLS",
    "host":"192.168.1.210",
    "port":21,
    "user":"AFAR",
    "password":"",
    "autoLogin":true
```

POST Response Body Sample

```
HTTP/1.1 201 Created Date: Thu, 04 Aug 2022 15:51:07 GMT Location:
/admin/v2/sites/76882fc7-3f55-4040-ae5f-2e645c12647b/connection-
profiles/92e9f684-5b87-47d3-816b-19644e639ae2 Content-Type:
application/vnd.api+json ETag: "24708EE" Content-Length: 1290 Cache-Control:
no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options:
nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src
'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer {
```

POST PowerShell Sample

```
##############################################
###POST Create New Connection Profile###
Write-Output " Create New Connection Profile"
Write-Output "------------------------------"
$update =
'{
  "data": {
    "id": "",
    "type": "connectionProfile",
    "attributes": {
      "name": "PS REQUEST Create connection Profile",
      "description": "Connection Profile Details",
      "testPath": "\test",
      "connectionSettings": {
        "protocol": "FTPSAuthTLS",
        "host": "192.168.1.210",
        "port": 21,
        "user": "AFAR",
        "password": "",
        "autoLogin": true,
        "certSettings": {
          "certPath": "C:\\Users\\Administrator\\Desktop\\AFAR SSL\\SSL Cert
```

Endpoint: /sites/{siteId}/connection-profiles/{connectionProfileID}

Note: Available as of EFT 8.1.0

(GET) GET Details for specific connection profile, (PATCH) update details for a specific connection profile, (DELETE) remove a specific connection profile.

- GET
- PATCH
- DELETE

Method & URL

```
GET https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles
```

GET Body Sample

```
### GET Details for specific connection profile####
###You can enter the Connection profile ID below or pass the value from a previous
request###
##@ConnectionProfileID = 31334739-2f41-4561-9d27-22e17c9b9362
GET https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles/{{ConnectionProfileID}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
HTTP/1.1 200 OK Date: Thu, 04 Aug 2022 16:11:35 GMT Location:
/admin/v2/sites/76882fc7-3f55-4040-ae5f-2e645c12647b/connection-
profiles/c9ea36ec-8a9e-440f-8c21-920eb3927732 Content-Type:
application/vnd.api+json ETag: "A50CA65F" Content-Length: 1289 Cache-Control:
no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options:
nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src
'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer
{ "data": { "id": "c9ea36ec-8a9e-440f-8c21-920eb3927732", "type":
"connectionProfile", "attributes": { "type": "Protocol", "name": "POST REQUEST
Create connection Profile", "description": "Connection Profile Details",
"connectionSettings": { "protocol": "FTPSAuthTLS", "user": "AFAR", "password":
"UpKUJq1sD4Yfb1Hz8ZFiRw==", "autoLogin": true, "testPath": "\test", "host":
"192.168.1.210", "port": 21, "SSLCertificate": { "certPath": "", "keyPath": "",
"passphrase": "UpKUJq1sD4Yfb1Hz8ZFiRw==" }, "trustedPubKey": "", "proxy": {
"use": false, "type": "FTP", "hostName": "", "username": "", "password":
"UpKUJq1sD4Yfb1Hz8ZFiRw==", "port": 21, "subType": 0, "separator": "@",
"customCommands": [] }, "socks": { "use": false, "type": "None", "hostName": "",
"port": 1080, "auth": false, "username": "", "password":
"UpKUJq1sD4Yfb1Hz8ZFiRw==" }, "advanced": { "numberOfConnectionRetries": 0,
"delayBetweenRetries": 30, "maxConcurrentThreads": 1, "connectionTimeout": 30,
```


GET PowerShell Sample

```
###Returns the deatails of the specified connection profile ###
Write-Output "Details of Connection Profile $profileId"
Write-Output "-----------------------------------------------------------------
----"
#$ConnectionProfileID = "Enter site ID"
$CPlist = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/connection-
Profiles/$ConnectionProfileID" -Method 'GET' -Headers $authHeader
Write-Output $CPlist | ConvertTo-Json -Depth 25
```

Method & URL

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/connection-
Profiles/{[ConnectionProfileID}}
```

PATCH Body Sample

```
### Update a Connection Profile ####
###You can enter the Connection profile ID below or pass the value from a previous
request###
##@ConnectionProfileID = 31334739-2f41-4561-9d27-22e17c9b9362
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles/{{ConnectionProfileID}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
 "data":{
   "type":"connectionProfile",
   "attributes":{
    "name":"Patch Connection Profile",
    "description":"Patch Connection Profile",
    "testPath":"/",
    "connectionSettings":{
     "protocol":"FTPSAuthTLS",
     "host":"192.168.1.210",
     "port":21,
     "user":"AFAR",
     "password":"pass",
     "autoLogin":false
     }
    }
```

PATCH Response Body Sample

```
HTTP/1.1 200 OK Date: Thu, 04 Aug 2022 18:33:38 GMT Location:
/admin/v2/sites/76882fc7-3f55-4040-ae5f-2e645c12647b/connection-
profiles/c9ea36ec-8a9e-440f-8c21-920eb3927732 Content-Type:
application/vnd.api+json ETag: "624A277A" Content-Length: 1408 Cache-
Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-
Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy:
no-referrer { "data": { "id": "c9ea36ec-8a9e-440f-8c21-920eb3927732",
"type": "connectionProfile", "attributes": { "type": "Protocol", "name":
"Patch Connection Profile", "description": "Patch Connection Profile",
"connectionSettings": { "protocol": "FTPSAuthTLS", "user": "AFAR",
"password": "wweZ1iVXRYBbX80z2T3JHg==", "autoLogin": false, "testPath":
"/", "host": "192.168.1.210", "port": 21, "SSLCertificate": { "certPath":
"C:\\Users\\administrator.TEST\\Desktop\\AFAR SSL\\SSL Cert User
AFAR.crt", "keyPath": "C:\\Users\\administrator.TEST\\Desktop\\AFAR
SSL\\SSL Cert User AFAR.key", "passphrase": "xamYEctkRdBRCxu0F5XqoQ==" },
"trustedPubKey": "", "proxy": { "use": false, "type": "FTP", "hostName": "",
```

PATCH PowerShell Sample

```
####Added 8/4/2022
### PATCH Connection Profile###
### User must obtain the SiteID and Connection Profile ID ###
Write-Output "PATCH Site Connection Profile"
Write-Output "-----------------------------"
$update =
'{
  "data": {
      "type": "connectionProfile",
      "attributes": {
        "name": "PS_Patch Connection Profile",
        "description": "PS_Patch Connection Profile",
        "testPath": "/",
        "connectionSettings": {
          "protocol": "FTPSAuthTLS",
          "host": "192.168.1.210",
          "port": 21,
          "user": "AFAR",
          "password": "pass",
          "autoLogin": false
          }
        }
```

Method & URL

DELETE
https://{{host}}/admin/v2/sites/{{Siteid}}/connection-Profiles/{{ConnectionProfileID}}

DELETE Body Sample

```
### DELETE specific connection profile####
DELETE  https://{{host}}/admin/v2/sites/{{Siteid}}/connection-
Profiles/{{ConnectionProfileID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Thu, 04 Aug 2022 18:52:32 GMT Content-
Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-
Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
```

DELETE PowerShell Sample

```
####Added 8/4/2022 ###
###### DELETE Connection Profile######
Write-Output "### DELETE specific Connection Profile###"
Write-Output "----------------------------------------"
$profileName = "PowerShell Example"
$Delete_Profile = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/connection-Profiles/$ConnectionProfileID" -Method
'DELETE' -Headers $authHeader
```

Endpoint: /experimental/site/templates/{templateName}

Returns the contents of the specified site template

Note: Available as of EFT 8.1.0

- GET
- PATCH

Method & URL

GET https://{{host}}/admin/v2/sites/{{Siteid}}/templates/{templateName}

GET Body Sample

```
#GET Site Templates -- ##
GET
https://{{host}}/admin/v2/sites/{{Siteid}}/templates/WorkspacesAdminAddedParticipantMsg.html HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 13:01:21 GMT Content-Type: application/vnd.api+json Content-Length: 370 Cache-Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer {
"data": "<html>\r\n<body>\r\n <p>Hello %USER.LOGIN%,</p>\r\n <p>The following <b>Enhanced File Transfer</b> Workspace has been shared with you: %FOLDER_NAME% (owner: %WS_OWNER_NAME%).</p>\r\n <p>Please use the following URL to access this Workspace:</p>\r\n <a href=\"%LINK%\">%LINK%</a><br/><br/>\r\n \r\n %WS_MESSAGE%<br/><br/>\r\n <hr/>\r\n</body>\r\n</html>" }
```

GET PowerShell Sample

```
####################################
#GET Site Template Details -- ##
Write-Output "GET Site Template Detail"
Write-Output "------------------------------"
#$siteID = "Enter site ID"
#$TemplateName= "WorkspacesAdminAddedParticipantMsg.html"
$TemplateDetails = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/templates/WorkspacesAdminAddedParticipantMsg.html" -Method 'GET' -Headers $authHeader
Write-Output $TemplateDetails | ConvertTo-Json -Depth 25
```

Method & URL

PATCH
https://{{host}}/admin/v2/sites/{{Siteid}}/templates/WorkspacesAdminAddedParticipantMsg.html

PATCH Body Sample

```
#Modify Site Template - Will append the site name to the file name should only be used for this site ##
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/templates/WorkspacesAdminAddedParticipantMsg.html HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
 "data":"<html>\r\n<body>\r\n <p>Update Template Example %USER.LOGIN%,</p>\r\n <p>The following <b>Enhanced File Transfer</b> Workspace has been shared with you: %FOLDER_NAME% (owner: %WS_OWNER_NAME%).</p>\r\n <p>Please use the following URL to access this Workspace:</p>\r\n <a href=\"%LINK%\">%LINK%</a><br/><br/>\r\n \r\n %WS_MESSAGE%<br/><br/>\r\n <hr/>\r\n</body>\r\n</html>"
}
```

PATCH Response Body Sample

```
HTTP/1.1 204 No Content Date: Fri, 05 Aug 2022 13:48:49 GMT Content-Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer
```

PATCH PowerShell Sample

```
####Added 8/4/2022
### Update Content of Template###
### Modify Site Template - Will append the site name to the file name should only be used for this site  ###
Write-Output "PATCH Site Connection Profile"
Write-Output "------------------------------"
$update =
'{
  "data": "<html>\r\n<body>\r\n  <p>PS1. Update Template Example %USER.LOGIN%,</p>\r\n  <p>The following <b>Enhanced File Transfer</b> Workspace has been shared with you: %FOLDER_NAME% (owner: %WS_OWNER_NAME%).</p>\r\n  <p>Please use the following URL to access this Workspace:</p>\r\n  <a href=\"%LINK%\">%LINK%</a><br/><br/>\r\n  \r\n %WS_MESSAGE%<br/><br/>\r\n  <hr/>\r\n</body>\r\n</html>"
}'
```

Endpoint:/sites/{siteID}/dmz

Note: Available as of EFT 8.1.0

(GET) Returns DMZ gateway settings from specified site and (PATCH) updates DMZ gateway settings

- GET
- PATCH

Method & URL

GET https://{{host}}/admin/v2/sites/{{Siteid}}/dmz

GET Body Sample

```
### GET SITE DMZ INFO ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/dmz HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{"data":{"type":"DMZGateway","attributes":{"enabled":false,"hosts":[],"po
rt":44500,"securePNC":{"enabled":false,"publicKeyPath":""},"ftp":{"enable
d":false,"port":21},"ftpsExpl":{"enabled":false,"port":21},"ftpsImpl":{"e
nabled":false,"port":990},"sftp":{"enabled":false,"port":22},"http":{"ena
bled":false,"port":80},"https":{"enabled":false,"port":443},"internalDoma
in":{"HTTPDomain":"","emailDomainPatterns":"","allowADorLDAPAuth":true,"i
sExclusiveADorLDAP":false,"isRequired2FAforInternalUsers":false,"SSLCerti
ficate":{"certPath":"","keyPath":"","passphrase":"UpKUJq1sD4Yfb1Hz8ZFiRw=
="}},"pasv":{"enabled":false,"listenIP":"0.0.0.0","portMin":28000,"portMa
x":30000},"remoteAdmin":{"enabled":false,"port":1100},"acceleration":{"en
```


GET PowerShell Sample

```
$siteID = $siteList.data[0].id

# get DMZ info
Write-Output "DMZ INFO"
Write-Output "-----"
$dmzList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/dmz" -Method
'GET' -Headers $authHeader
Write-Output $dmzList | ConvertTo-Json
```

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/dmz
```

PATCH Body Sample

```
### PATCH (UPDATE) DMZ INFO ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/dmz HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "DMZGateway",
    "attributes": {
      "hosts":
      [
        "10.91.160.102"
      ],
      "port":"44500",
      "enabled": true,
      "ftpEnabled": false,
      "ftpsEnabled": true,
      "ftpsExpEnabled": true,
      "sftpEnabled": false,
      "ftpPort": 21,
      "ftpsPort": 990,
      "httpsEnabled": true,
      "adminEnabled": true,
      "adminPort": 1100
    }
  }
}
###
```

PATCH Response Body Sample

```
{"data":{"type":"DMZGateway","attributes":{"enabled":true,"hosts":["10.91
.160.102"],"port":44500,"securePNC":{"enabled":false,"publicKeyPath":""},
"ftp":{"enabled":false,"port":21},"ftpsExpl":{"enabled":false,"port":21},
"ftpsImpl":{"enabled":false,"port":990},"sftp":{"enabled":false,"port":22
},"http":{"enabled":false,"port":80},"https":{"enabled":false,"port":443}
,"internalDomain":{"HTTPDomain":"","emailDomainPatterns":"","allowADorLDA
PAuth":true,"isExclusiveADorLDAP":false,"isRequired2FAforInternalUsers":f
alse,"SSLCertificate":{"certPath":"","keyPath":"","passphrase":"UpKUJq1sD
4Yfb1Hz8ZFiRw=="}},"pasv":{"enabled":false,"listenIP":"0.0.0.0","portMin"
:28000,"portMax":30000},"remoteAdmin":{"enabled":false,"port":1100},"acce
```


PATCH PowerShell Sample

```
##Patch SITE DMZ settings
Write-Output "Site DMZ PATCH"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "DMZGateway",
    "attributes": {
      "hosts":
      [
        "10.91.160.102"
      ],
      "port":"44500",
      "enabled": true,
      "ftpEnabled": false,
      "ftpsEnabled": true,
      "ftpsExpEnabled": true,
      "sftpEnabled": false,
      "ftpPort": 21,
      "ftpsPort": 990,
      "httpsEnabled": true,
      "adminEnabled": true,
      "adminPort": 1100
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchDMZReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/dmz" -
Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $patchDMZReturn | ConvertTo-Json
```

Security REST API

Endpoint: /lists/security/tls/algorithms

Returns a list of tls algorithms

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/lists/security/tls/algorithms

GET Body Sample

```
###
##Get Server TLS Security Settings
GET https://{{host}}/admin/v2/lists/security/tls/algorithms HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{ "data": { "attributes": { "resultingCipherList": [ "ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384", "DHE-RSA-AES256-GCM-SHA384", "ECDHE-ECDSA-CHACHA20-POLY1305", "ECDHE-RSA-CHACHA20-POLY1305", "DHE-RSA-CHACHA20-POLY1305", "ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-RSA-AES128-GCM-SHA256", "DHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-SHA384",
```


GET PowerShell Sample

```
###
#GET TLS ALOGRITHMS
Write-Output "Get EFT TLS ALGORITHMS"
$serverNodeID = "DTY2019WinServe"

Write-Output "Server Node: $serverNodeID"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri
"$baseURL/v2/lists/security/tls/algorithms" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Endpoint: /lists/security/ssh/algorithms

Returns a list of ssh algorithms

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/lists/security/ssh/algorithms

GET Body Sample

```
###
##Get Server SSH Security Settings
GET https://{{host}}/admin/v2/lists/security/ssh/algorithms HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{ "data": { "attributes": { "algorithms": { "ciphers": [ "aes256-gcm@openssh.com", "aes256-ctr", "aes256-cbc", "rijndael-cbc@lysator.liu.se", "twofish256-cbc", "twofish-cbc", "aes192-ctr", "aes192-cbc", "aes128-gcm@openssh.com", "aes128-ctr", "aes128-cbc", "twofish128-cbc",
```

GET PowerShell Sample

```
###
#GET SSH ALOGRITHMS
Write-Output "Get EFT SSH ALGORITHMS"
$serverNodeID = "DTY2019WinServe"

Write-Output "Server Node: $serverNodeID"
Write-Output "-----"
$serverAdminDetails = Invoke-RestMethod -Uri
"$baseURL/v2/lists/security/ssh/algorithms" -Method 'GET' -Headers $authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Endpoint: /lists/security/tls/ciphers/{cipherString}

Returns a list of resulting ciphers

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/lists/security/tls/ciphers/{cipherString}

GET Body Sample

```
###
##Get Server TLS Ciphers Settings
GET https://{{host}}/admin/v2/lists/security/tls/ciphers/"aes-ctr"
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "attributes": { "resultingCipherList": [ "ECDHE-ECDSA-AES256-
GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384", "DHE-RSA-AES256-GCM-SHA384",
"ECDHE-ECDSA-CHACHA20-POLY1305", "ECDHE-RSA-CHACHA20-POLY1305", "DHE-RSA-
CHACHA20-POLY1305", "ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-RSA-AES128-
GCM-SHA256", "DHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-SHA384",
```

GET PowerShell Sample

```
###
#GET TLS CIPHERS
Write-Output "Get EFT TLS CIPHERS"
$serverNodeID = "DTY2019WinServe"
$cipherId = "aes-ctr"

Write-Output "Server Node: $serverNodeID"
Write-Output "-----""
$serverAdminDetails = Invoke-RestMethod -Uri
"$baseURL/v2/lists/security/tls/ciphers/$cipherID -Method 'GET' -Headers
$authHeader
Write-Output $serverAdminDetails | ConvertTo-Json -Depth 10
```

Login/Logout REST API

Endpoint: /logout

Logs out of current session.

- POST

Method & URL

POST https://[server URL]:[port]/admin/v2/logout

POST Body Sample

```
POST https://{{host}}/admin/v2/logout HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

POST Response Body Sample

```
HTTP/1.1 200 OK Date: Wed, 10 Aug 2022 20:10:28 GMT Content-Length: 0
Set-Cookie: websessionid=xxxxxx; expires=Tuesday, 10-Aug-21 20:10:28 GMT;
path=/; secure; HttpOnly; SameSite=Strict Cache-Control: no-cache, no-
store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-
Protection: 1; mode=block Content-Security-Policy: default-src 'self'
'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer
```

POST PowerShell Sample

```
# POST - logout
$auth = Invoke-RestMethod -Uri "$baseURL/v2/logout" -Method 'POST' -Body
$authBody -Headers $authHeader
#
```

Keep-Alive REST API

Endpoint: /keep-alive

Note: Available as of EFT 8.1.0

Extends current session.

- HEAD

Method & URL

HEAD https://[server URL]:[port]/admin/v2/keep-alive

HEAD Body Sample

```
##Get Server keep alive
HEAD https://{{host}}/admin/v2/keep-alive HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

HEAD Response Body Sample

```
HTTP/1.1 200 OK Date: Mon, 21 Feb 2022 22:17:46 GMT Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-
Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-
Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-
Policy: no-referrer
```

HEAD PowerShell Sample

```
# keep-alive
Write-Output "Keep Alive"
Write-Output "----"
$keepAlive = Invoke-RestMethod -Uri "$baseURL/v2/keep-alive" -Method 'HEAD' -
Headers $authHeader
```

Users REST API

Endpoint: /sites/{siteId}/users

Note: Available as of EFT 8.1.0

Returns a list of users for specific site, create user(s) for a specific site.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/users

GET Body Sample

```
### GET SITE USERS ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": [ { "attributes": { "accountEnabled": "inherit",
"agreementToTermsOfService": "unknown", "as2": { "inbound": { "enabled":
"inherit" }, "outbound": { "enabled": "inherit" } }, "changePassword": {
"enabled": "inherit", "value": {
"changeAdminProvidedPasswordUponFirstUse": "inherit",
```

GET PowerShell Sample

```
# get sites
Write-Output "Site"
Write-Output "----"
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites" -Method 'GET' -Headers
$authHeader
Write-Output $siteList | ConvertTo-Json
foreach ($site in $siteList.data)
{
    Write-Output ("Site  $($site.id): $($site.attributes.name)")
}

$siteID = $siteList.data[0].id

# get users
Write-Output "Users"
Write-Output "-----"
$userList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users" -Method
'GET' -Headers $authHeader
Write-Output $userList | ConvertTo-Json
foreach ($user in $userList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

POST https://[server URL]:[port]/admin/v2/ sites/{siteId}/users

POST Body Sample

```
### ADD SITE USER ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "user",
    "attributes": {
      "loginName": "TestUser1",
      "password": {
        "type": "Disabled",
        "value": "Alaska12#"
      },
      "accountEnabled": "inherit",
      "expiration": {
        "enabled": false,
        "value": {
          "date": {}
        }
      },
      "personal": {
        "name": "Test User",
        "description": null,
        "email": null,
```

POST Response Body Sample


```
"data": { "attributes": { "accountEnabled": "inherit",
"agreementToTermsOfService": "unknown", "as2": { "inbound": { "enabled":
"inherit" }, "outbound": { "enabled": "inherit" } }, "changePassword": {
"enabled": "inherit", "value": {
"changeAdminProvidedPasswordUponFirstUse": "inherit",
"mustChangePassword": false, "passwordExpiration": { "enabled": true,
"value": { "maxAgeDays": 90, "emailUpon": true, "remindPrior": {
"enabled": false, "value": { "daysBefore": 5, "emailUser": true } } } } }
}, "connectionTimeout": { "enabled": "inherit", "value": { "maxSec": 0 }
},
```


POST PowerShell Sample

```
Write-Output "Add User POST"
Write-Output "-----"
$update =
'{
  "data": {
    "type": "user",
    "attributes": {
      "loginName": "TestUser2",
      "password": {
        "type": "Disabled",
        "value": "Alaska12#"
      },
      "accountEnabled": "inherit",
      "expiration": {
        "enabled": false,
        "value": {
          "date": {}
        }
      },
      "personal": {
        "name": "Test User",
        "description": null,
        "email": null,
        "DUNS": null,
        "phone": null,
        "mobile": null,
        "pager": null,
        "fax": null,
        "company": null,
        "partnerId": null,
        "custom1": null,
        "custom2": null,
        "custom3": null,
        "comments": null
      },
      "isEuDataSubject": "unknown",
      "consentToPrivacyPolicy": "unknown",
      "agreementToTermsOfService": "unknown",
      "homeFolder": {
        "enabled": "yes",
        "value": {
          "path": null
        }
      },
      "hasHomeFolderAsRoot": "inherit",
      "externalAuthentication": "inherit",
      "ftp": {
        "enabled": "inherit",
        "value": {
          "enableFxp": "inherit",
          "enableNoop": "inherit",
          "enableComb": "inherit",
          "enableXcrc": "inherit",
          "enableZlib": "inherit",
          "banner": {
            "message": "",
            "usage": "useDefault"
          }
        }
      },
      "ftps": {
```

Endpoint: /sites/{siteid}/users/{userid}

Returns, updates, and deletes user account details.

- GET
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}

GET Body Sample

```
### GET SITE SPECIFIC USER ###
# @name usersList
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###

@Usersid = {{usersList.response.body.$.data[0].id}}
###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{ "data": { "attributes": { "accountEnabled": "inherit",
"agreementToTermsOfService": "unknown", "as2": { "inbound": { "enabled":
"inherit" }, "outbound": { "enabled": "inherit" } }, "changePassword": {
"enabled": "inherit", "value": {
"changeAdminProvidedPasswordUponFirstUse": "inherit",
"mustChangePassword": false, "passwordExpiration": { "enabled": true,
"value": { "maxAgeDays": 90, "emailUpon": true, "remindPrior": {
"enabled": false, "value": { "daysBefore": 5, "emailUser": true
```


GET PowerShell Sample

```
# get a specific users information
Write-Output "Users"
Write-Output "-----"
$userList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users" -Method
'GET' -Headers $authHeader
Write-Output $userList | ConvertTo-Json
foreach ($user in $userList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}

$userid = $userList.data[0].id

# get user's data
Write-Output "Users"
Write-Output "-----"
$userList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users/$userid" -
Method 'GET' -Headers $authHeader
Write-Output $userList | ConvertTo-Json
foreach ($user in $userList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/

PATCH Body Sample

```
@Usersid = {{usersList.response.body.$.data[0].id}}
###
### UPDATE A USERS PERSONAL INFORMATION ###
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}/
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "user",
    "attributes": {
      "personal": {
        "name": "MR JONES",
        "description": “MANAGER",
        "email": "user@example.com",
        "duns": "",
        "phone": "",
        "mobile": "2107221301",
        "pager": "",
        "fax": "",
        "company": "",
        "partnerId": "",
        "custom1": "1234",
        "custom2": "5678",
        "custom3": "abcd",
        "comments": "Does this work?"
      },
      "isEuDataSubject": "yes",
      "consentToPrivacyPolicy": "grantedExplicit",
      "agreementToTermsOfService": "agreedExplicit"
    }
  }
```

PATCH Response Body Sample

```
{ "data": { "attributes": { "accountEnabled": "inherit",
"agreementToTermsOfService": "agreedExplicit", "as2": { "inbound": {
"enabled": "inherit" }, "outbound": { "enabled": "inherit" } },
"changePassword": { "enabled": "inherit", "value": {
"changeAdminProvidedPasswordUponFirstUse": "inherit",
"mustChangePassword": false, "passwordExpiration": { "enabled": true,
"value": { "maxAgeDays": 90, "emailUpon": true, "remindPrior": {
"enabled": false, "value": { "daysBefore": 5, "emailUser": true } } } } }
```

PATCH PowerShell Sample

```
##UPDATE USERS
Write-Output "Update user data"
Write-Output "-----"
$update =
'{
    "data": {
       "type": "user",
       "attributes": {
       "accountEnabled": "no"

       }
      }

}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$PatchReturn = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/users/$userid" -Method 'PATCH' -Headers $authHeader
-Body $update
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/

DELETE Body Sample

```
### REMOVE THE USER ### (userOnly, userAndHomeFolder)
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "parameters": {
        "scope": "userAndHomeFolder"
    }
}
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Fri, 04 Feb 2022 21:00:36 GMT Content-
Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-
Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
```

DELETE PowerShell Sample

```
$update =
'{
    "parameters": {
        "scope": "userAndHomeFolder"
    }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
# delete
Write-Output "Delete User"
Write-Output "-----"
$deleteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/users/$userid"
-Method 'DELETE' -Headers $authHeader -Body $update
Write-Output $deleteList | ConvertTo-Json
foreach ($user in $deleteList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteid}/users/{userid}/as2inbound

Returns and updates user inbound AS2 parameters

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/as2inbound

GET Body Sample

```
# @name usersList
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###

@Usersid = {{usersList.response.body.$.data[0].id}}
###
GET
https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}/as2inbound
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "attributes": { }, "relationships": {
"transactionFailedCommand": { "data": null },
"transactionSuccessCommand": { "data": null } }, "type": "AS2Inbound" } }
```

GET PowerShell Sample

```powershell
$userid = $userList.data[0].id

# get users
Write-Output "Specific User AS2inbound information"
Write-Output "-----"
$userList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/users/$userid/as2inbound" -Method 'GET' -Headers
$authHeader
Write-Output $userList | ConvertTo-Json
foreach ($user in $userList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/as2inbound

PATCH Body Sample

```
###
PATCH
https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}/as2inbound
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "AS2Inbound",
    "attributes": {
      "myId": "AS2_1",
      "partnerId": "AS2_2"
    }
```

PATCH Response Body Sample

```
{
  "data": {
    "attributes": {
      "allowedEncryptionAlgorithms": [
      ],
      "allowedSignatureAlgorithms": [
      ],
      "authenticationType": "usernamePassword",
      "contentCollision": "reject",
      "doNotSend100Continue": false,
      "folderToMoveDataTo": "",
      "mdnSendAttemptDelaySeconds": 30,
```

PATCH PowerShell Sample

```
$update =
'{
  "data": {
    "type": "AS2Inbound",
    "attributes": {
      "myId": "AS2_1",
      "partnerId": "AS2_4",
      "partnerCertificateFilePath":
"C:\\Users\\DYelacic1951\\Desktop\\certs\\ssl.crt"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
# update / patch
Write-Output "Update User specific as2inbound information"
Write-Output "-----"
$as2InboundList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/users/$userid/as2inbound" -Method 'PATCH' -Headers
$authHeader -Body $update
Write-Output $as2InboundList | ConvertTo-Json
foreach ($user in $as2InboundList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteid}/users/{userid}/as2outbound

Returns and updates user outbound AS2 parameters

- GET
- PATCH

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/as2outbound

GET Body Sample

```
# @name usersList
GET https://{{host}}/admin/v2/sites/{{Siteid}}/users HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###

@Usersid = {{usersList.response.body.$.data[0].id}}
###
GET
https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}/as2outbound
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
{ "data": { "attributes": { }, "relationships": { }, "type":
"AS2Outbound" } }
```

GET PowerShell Sample

```
Write-Output "Users specific as2outbound information"
Write-Output "-----"
$as2outList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/users/$userid/as2outbound" -Method 'GET' -Headers
$authHeader
Write-Output $as2outList | ConvertTo-Json
foreach ($user in $as2outList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/as2outbound

PATCH Body Sample

```
###
PATCH
https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{Usersid}}/as2outbound
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "AS2outbound",
    "attributes": {
      "myId": "AS2_1",
      "partnerId": "AS2_4",
    "hotFolderPath": "C:\\Users\\DYelacic1951\\Desktop\\HOTBOX\\"
    }
  }
```

PATCH Response Body Sample

```
{ "data": { "attributes": { }, "relationships": { }, "type":
"AS2Outbound" } }
```

PATCH PowerShell Sample

```
$update =
'{
  "data": {
    "type": "AS2outbound",
    "attributes": {
      "myId": "AS2_1",
      "partnerId": "AS2_4",
        "hotFolderPath": "C:\\Users\\DYelacic1951\\Desktop\\HOTBOX\\"
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
# update / patch
Write-Output "Update User specific as2outbound information"
Write-Output "-----"
$as2outboundList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/users/$userid/as2outbound" -Method 'PATCH' -Headers
$authHeader -Body $update
Write-Output $as2outboundList | ConvertTo-Json
foreach ($user in $as2outboundList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteid}/users/{userid}/counters

Returns user account statistics (As of EFT 8.1 the response will include this data pair "timePasswordChanged")

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/users/{userid}/counters

GET Body Sample

```
#### GET USER DETAILS COUNTERS ####
## Must obtain User_ID##

GET https://{{host}}/admin/v2/sites/{{Siteid}}/users/{{UserID}}/counters HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 17:43:54 GMT Content-Type:
application/vnd.api+json Content-Length: 264 Cache-Control: no-cache, no-
store, must-revalidate Expires: -1 X-Content-Type-Options: nosniff X-XSS-
Protection: 1; mode=block Content-Security-Policy: default-src 'self'
'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy: no-referrer


{ "data": { "attributes": { "isConnected": false, "isLocked": false,
"lastModifiedBy": "admin", "timeCreated": "2022-08-04 01:23:35 PM",
"timeLastConnected": null, "timeLastModified": "2022-08-04 01:23:35 PM",
"timePasswordChanged": "2022-08-04 01:23:35 PM" }, "type": "userCounters"
} }
```

GET PowerShell Sample

```
$userid = $userList.data[0].id

# get users counters
Write-Output "Users counters"
Write-Output "-----"
$userList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/users/$userid/counters" -Method 'GET' -Headers
$authHeader
Write-Output $userList | ConvertTo-Json
foreach ($user in $userList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Filesystem REST API

Endpoint: /sites/{siteId}/filesystem/folders

Returns folder (updated on EFT 8.1, it now includes the Upload Quota Settings)

- GET

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders

GET Body Sample

```
@Siteid = {{siteList.response.body.$.data[0].id}}
###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 16:59:16 GMT Content-Type:
application/vnd.api+json ETag: "B7E6B8C3" Content-Length: 529 Cache-
Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-
Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy:
no-referrer

{"data": {"attributes": {"name": "", "subFolders": ["anonymous", "Bin",
"Incoming", "Pub", "Usr"], "target": {"type": "winFolder", "winFolder": {
"path": "C:\\InetPub\\EFTRoot\\MySite\\" }}, "uploadQuota": null }, "id":
"%2F", "links": {"self": "/admin/v2/sites/e82de253-b8ec-4b70-a72d-
d017c3317f01/filesystem/folders/%252F" }, "relationships": {
"inheritedPermissions": {"meta": {"name": "inherited permissions" }},
"permissions": {"links": {"related": "/admin/v2/sites/e82de253-b8ec-
```

GET PowerShell Sample

```
$userid = $userList.data[0].id

# get users counters
Write-Output "filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders" -Method 'GET' -Headers
$authHeader
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}

Returns folder settings, updates folder settings, creates folders, and deletes folders (updated on EFT 8.1, it now includes the Upload Quota Settings)

- GET
- POST
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}

GET Body Sample

```
##### GET the Folder structure and settings for a specifc User  #########
@User_Folder_ID = AFAR
GET
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2F{{User_Folder_ID}}%2F
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 17:04:14 GMT Content-Type:
application/vnd.api+json ETag: "95FFEAF1" Content-Length: 470 Cache-
Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-
Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy:
no-referrer
{ "data": { "attributes": { "name": "AFAR", "subFolders": [], "target":
null, "uploadQuota": null }, "id": "%2Fusr%2FAFAR%2F", "links": { "self":
"/admin/v2/sites/e82de253-b8ec-4b70-a72d-
d017c3317f01/filesystem/folders/%252Fusr%252FAFAR%252F" },
"relationships": { "inheritedPermissions": { "meta": { "name": "inherited
permissions" } }, "permissions": { "links": { "related":
"/admin/v2/sites/e82de253-b8ec-4b70-a72d-
d017c3317f01/filesystem/folders/%252Fusr%252FAFAR%252F/permissions" } } }
```

GET PowerShell Sample

```powershell
# get filesystem folders
Write-Output "filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2Fusr%2F" -Method 'GET' -
Headers $authHeader
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}

POST Body Sample

```
###
POST
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2fusr%2fdy
elacic%2f/folders HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
    "data": {
        "type": "folder",
        "id": "%2Fbiohazard%2F",
        "attributes": {
            "name": "biohazard",
            "target": "c:/temp"
        }
    }
}
```

POST Body Sample - Example II – including Upload Quotas

```
##### POST REQUEST TO CREATE A FOLDER WITH UPLOAD QUOTA ENABLED #########
@User_Folder = afar
POST
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2F{{User_Folder}}%2F/fo
lders HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
 "data":{
  "type":"folder",
  "attributes":{
   "name":"Folder4",
   "subFolder":"Folder4",
  "uploadQuota":{
    "emailsToReportToOnExceed":[
     "gsqaaf1@gmail.com",
     "gsqaaf2@gmail.com"
    ],
    "enabled":true,
    "limitMBytes":150,
    "usedMBytes":0
   }
  }
 }
```

POST Response Body Sample


```
{ "data": { "attributes": { "name": "biohazard", "subFolders": [],
"target": "c:/temp" }, "id": "%2Fusr%2Fdyelacic%2Fbiohazard%2F", "links":
{ "self": "/Admin/v2/sites/f1e58e70-926f-4786-877b-
cf62abfdf0db/filesystem/folders/%252Fusr%252Fdyelacic%252Fbiohazard%252F"
}, "relationships": { "inheritedPermissions": { "meta": { "name":
"inherited permissions" } }, "permissions": { "links": { "related":
"/Admin/v2/sites/f1e58e70-926f-4786-877b-
cf62abfdf0db/filesystem/folders/%252Fusr%252Fdyelacic%252Fbiohazard%252F/
```


POST PowerShell Sample

```
$update =
'{
    "data": {
        "type": "folder",
        "id": "%2Fmetallica2%2F",
        "attributes": {
            "name": "metallica2",
            "target": "c:/util"
        }
    }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 20
# update filesystem folders
Write-Output "filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2fusr%2fFranklin%2f" -Method
'POST' -Headers $authHeader -Body $update
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}

PATCH Body Sample

```
#
# change the path to where this virtual folder points
#
###
PATCH
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2Fte
st_user_sql%2Fmetallica%2F HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "attributes": {
      "name": "metallica",
      "subFolders": [],
      "target": {
        "type": "winFolder",
        "winFolder": {
          "path": "C:\\temp"
        }
```

PATCH Response Body Sample

```
HTTP/1.1 200 OK Date: Thu, 18 Aug 2022 13:31:59 GMT Content-Type:
application/vnd.api+json ETag: "B0A1B271" Content-Length: 590 Cache-
Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-
Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy:
no-referrer { "data": { "attributes": { "name": "metallica",
"subFolders": [], "target": { "type": "winFolder", "winFolder": { "path":
"C:\\temp" } }, "uploadQuota": null }, "id":
"%2Fusr%2Ftest_user_sql%2Fmetallica%2F", "links": { "self":
```

PATCH PowerShell Sample

```
#
# renaming the virtual folder name
#
$update =
'{

  "data": {
    "attributes": {
      "name": "metallica",
      "subFolders": [],
      "target": {
        "type": "winFolder",
        "winFolder": {
          "path": "C:\\temp"
        }
      },
      "uploadQuota": null
    },
    "id": "%2Fusr%2Ftest_user_sql%2Fmetallica%2F",
    "type": "folder"
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 20
# update filesystem folders
Write-Output "patch filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2fusr%2fdyelacic%2fmetallica%2f
" -Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}

DELETE Body Sample

```
###
DELETE
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2FFr
anklin%2F HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Thu, 10 Feb 2022 14:49:46 GMT Content-
Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-
Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
Write-Output "delete filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2Fusr%2Fdyelacic%2F" -Method
'DELETE' -Headers $authHeader
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/folders

Creates physical or virtual sub-folder

- POST

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}/folders

POST Body Sample

```
#
# creating a physical sub folder below the users home folder
#
###
POST
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2Fdy
elacic%2F/folders HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "folder",
    "attributes": {
      "name": "tuneroom",
      "subFolder": "tuneroom"
    }
  }
}
###
```

POST Response Body Sample

```
{ "data": { "attributes": { "name": "tuneroom", "subFolders": [],
"target": null }, "id": "%2Fusr%2Fdyelacic%2Ftuneroom%2F", "links": {
"self": "/Admin/v2/sites/f1e58e70-926f-4786-877b-
cf62abfdf0db/filesystem/folders/%252Fusr%252Fdyelacic%252Ftuneroom%252F"
}, "relationships": { "inheritedPermissions": { "meta": { "name":
"inherited permissions" } }, "permissions": { "links": { "related":
"/Admin/v2/sites/f1e58e70-926f-4786-877b-
cf62abfdf0db/filesystem/folders/%252Fusr%252Fdyelacic%252Ftuneroom%252F/p
ermissions" } } }, "type": "folder" } }
```

POST PowerShell Sample

```
#
# create physical sub folder below users home folder
#
$update =
'{
    "data": {
        "type": "folder",
        "attributes": {
            "name": "sunroom",
            "subFolder": "sunroom"
        }
    }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 20
# create filesystem folders
Write-Output "create sub folder"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2fusr%2fdyelacic%2f/folders" -
Method 'POST' -Headers $authHeader -Body $update
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/permissions

Returns a list of permissions for a specific folder, adding existing permissions to a specific folder.

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}/permissions

GET Body Sample

```
# get folder permissions
#
###
GET
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2Fdy
elacic%2F/permissions HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
{ "data": [ { "attributes": { "canAppendFile": true,
"canCreateSubfolder": true, "canDeleteFile": true, "canDeleteSubfolder":
true, "canDownloadFile": true, "canList": true,
"canRenameFileOrSubfolder": true, "canSeeHiddenFileOrSubfolder": true,
"canSeeInParentList": true, "canSeeReadOnlyFileOrSubfolder": true,
"canUploadFile": true }, "links": { "self": "/Admin/v2/sites/f1e58e70-
926f-4786-877b-
cf62abfdf0db/filesystem/folders/%252Fusr%252Fdyelacic%252F/permissions/us
er-04dcfd20-fc73-41d0-a0d8-62d1706e6281" }, "relationships": { "trustee":
{ "data": { "id": "04dcfd20-fc73-41d0-a0d8-62d1706e6281", "meta": {
"name": "dyelacic" }, "type": "user" }, "links": { "related":
"/Admin/v2/sites/f1e58e70-926f-4786-877b-cf62abfdf0db/users/04dcfd20-
```


GET PowerShell Sample

```
#
# get filesystem folders permissions
Write-Output "filesystem folders"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2Fusr%2Fdyelacic%2f/permissions
" -Method 'GET' -Headers $authHeader
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}/permissions

POST Body Sample

```
###
#Add / Link folder to an existing user permissions group.

POST
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2Ftest_user_sql%2Fspam%2F/permissions HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data":
    {
      "type": "folderPermissions",
      "attributes": {
        "canAppendFile": true,
        "canCreateSubfolder": true,
        "canDeleteFile": true,
        "canDeleteSubfolder": true,
        "canDownloadFile": true,
        "canList": true,
        "canRenameFileOrSubfolder": true,
        "canSeeHiddenFileOrSubfolder": true,
        "canSeeInParentList": true,
        "canSeeReadOnlyFileOrSubfolder": true,
        "canUploadFile": false
      },
      "relationships": {
        "trustee": {
          "data": {
            "type": "userGroup",
            "id": " b8448b77-01d8-47d5-8ee7-9f407c95e39f",
            "meta": {
              "name": "Guests"
            }
          }
        }
      }
    }
 }
###
```

POST Response Body Sample

```
HTTP/1.1 201 Created Date: Thu, 18 Aug 2022 19:32:43 GMT Location:
/admin/v2/sites/7c2d15e3-e151-4029-8aa2-
d4475296ba1c/filesystem/folders/%252Fusr%252Ftest_user_sql%252Fspam%252F/
permissions/group-b8448b77-01d8-47d5-8ee7-9f407c95e39f Content-Type:
application/vnd.api+json ETag: "C5020903" Content-Length: 774 Cache-
Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-
Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy:
no-referrer { "data": { "attributes": { "canAppendFile": true,
"canCreateSubfolder": true, "canDeleteFile": true, "canDeleteSubfolder":
true, "canDownloadFile": true, "canList": true,
"canRenameFileOrSubfolder": true, "canSeeHiddenFileOrSubfolder": true,
"canSeeInParentList": true, "canSeeReadOnlyFileOrSubfolder": true,
"canUploadFile": false }, "links": { "self": "/admin/v2/sites/7c2d15e3-
e151-4029-8aa2-
d4475296ba1c/filesystem/folders/%252Fusr%252Ftest_user_sql%252Fspam%252F/
permissions/group-b8448b77-01d8-47d5-8ee7-9f407c95e39f" },
"relationships": { "trustee": { "data": { "type": "userGroup", "id":
"b8448b77-01d8-47d5-8ee7-9f407c95e39f", "meta": { "name": "Guests" } },
"links": { "related": "/admin/v2/sites/7c2d15e3-e151-4029-8aa2-
```

POST PowerShell Sample

```
#
# Add an existing user permissions group to a folder
$update =
'{

  "data":
    {
      "type": "folderPermissions",
      "attributes": {
        "canAppendFile": true,
        "canCreateSubfolder": true,
        "canDeleteFile": true,
        "canDeleteSubfolder": true,
        "canDownloadFile": true,
        "canList": true,
        "canRenameFileOrSubfolder": true,
        "canSeeHiddenFileOrSubfolder": true,
        "canSeeInParentList": true,
        "canSeeReadOnlyFileOrSubfolder": true,
        "canUploadFile": false
      },
      "relationships": {
        "trustee": {
          "data": {
            "type": "userGroup",
            "id": "b8448b77-01d8-47d5-8ee7-9f407c95e39f",
            "meta": {
              "name": "Guests"
            }
          }
        }
      }
    }
 }'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
# add sub folder permissions
Write-Output "add sub folder permissions"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2fusr%2fdyelacic%2ftuneroom%2f/
permissions" -Method 'POST' -Headers $authHeader -Body $update
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Endpoint: /sites/{siteId}/filesystem/folders/{folderid}/permissions/{folderpermid}

Returns, updates, and deletes permissions on folder

- GET

- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}/permissions/{folderpermid}

GET Body Sample

```
# get the permissions for a specific folder
#
###
GET
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2Fdyelacic%2Fsunroom%2F/permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{ "data": { "attributes": { "canAppendFile": true, "canCreateSubfolder": true, "canDeleteFile": true, "canDeleteSubfolder": true, "canDownloadFile": false, "canList": true, "canRenameFileOrSubfolder": true, "canSeeHiddenFileOrSubfolder": true, "canSeeInParentList": true, "canSeeReadOnlyFileOrSubfolder": true, "canUploadFile": true }, "links": { "self": "/Admin/v2/sites/f1e58e70-926f-4786-877b-cf62abfdf0db/filesystem/folders/%252Fusr%252Fdyelacic%252Fsunroom%252F/permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281" }, "relationships": { "trustee": { "data": { "id": "04dcfd20-fc73-41d0-a0d8-62d1706e6281", "meta": { "name": "dyelacic" }, "type": "user" }, "links": { "related": "/Admin/v2/sites/f1e58e70-926f-4786-877b-cf62abfdf0db/users/04dcfd20-fc73-41d0-a0d8-62d1706e6281" } } }, "type": "folderPermissions" } }
```


GET PowerShell Sample

```powershell
# get the folders permission
# get filesystem folders permissions
Write-Output "filesystem folders permissions"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2Fusr%2Fdyelacic%2fsunroom%2f/p
ermissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281" -Method 'GET' -Headers
$authHeader
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}/permissions/{folderpermid}

PATCH Body Sample

```
# change / update folder permissions
###
PATCH
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2Fdy
elacic%2Fsunroom%2F/permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
    "type": "folderPermissions",
    "attributes": {
      "canUploadFile": false,
      "canDownloadFile": true,
      "canDeleteFile": false,
      "canRenameFileOrSubfolder": true,
      "canAppendFile": true,
      "canDeleteSubfolder": false,
      "canCreateSubfolder": true,
      "canSeeHiddenFileOrSubfolder": true,
      "canSeeReadOnlyFileOrSubfolder": true,
      "canSeeInParentList": true,
      "canList": true
    }
  }
```

PATCH Response Body Sample

```
{ "data": { "attributes": { "canAppendFile": true, "canCreateSubfolder":
true, "canDeleteFile": false, "canDeleteSubfolder": false,
"canDownloadFile": true, "canList": true, "canRenameFileOrSubfolder":
true, "canSeeHiddenFileOrSubfolder": true, "canSeeInParentList": true,
"canSeeReadOnlyFileOrSubfolder": true, "canUploadFile": false }, "links":
{ "self": "/Admin/v2/sites/f1e58e70-926f-4786-877b-
cf62abfdf0db/filesystem/folders/%252Fusr%252Fdyelacic%252Fsunroom%252F/pe
rmissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281" }, "relationships":
{ "trustee": { "data": { "id": "04dcfd20-fc73-41d0-a0d8-62d1706e6281",
"meta": { "name": "dyelacic" }, "type": "user" }, "links": { "related":
"/Admin/v2/sites/f1e58e70-926f-4786-877b-cf62abfdf0db/users/04dcfd20-
fc73-41d0-a0d8-62d1706e6281" } } }, "type": "folderPermissions" } }
```


PATCH PowerShell Sample

```
# change folder permissions
$update =
'{
  "data": {
    "type": "folderPermissions",
    "attributes": {
      "canUploadFile": false,
      "canDownloadFile": true,
      "canDeleteFile": false,
      "canRenameFileOrSubfolder": true,
      "canAppendFile": true,
      "canDeleteSubfolder": false,
      "canCreateSubfolder": true,
      "canSeeHiddenFileOrSubfolder": true,
      "canSeeReadOnlyFileOrSubfolder": true,
      "canSeeInParentList": true,
      "canList": true
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
# change folder permissions
Write-Output "change folder permissions"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2fusr%2fdyelacic%2ftuneroom%2f/
permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281" -Method 'PATCH' -
Headers $authHeader -Body $update
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/filesystem/folders/{folderid}/permissions/{folderpermid}

DELETE Body Sample

```
# delete folder permissions

###
DELETE
https://{{host}}/admin/v2/sites/{{Siteid}}/filesystem/folders/%2Fusr%2Fdy
elacic%2Fsunroom%2F/permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Fri, 11 Feb 2022 22:06:08 GMT Content-
Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-
Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
#
# delete folder permissions

Write-Output "delete folders permissions"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri
"$baseURL/v2/sites/$siteID/filesystem/folders/%2Fusr%2Fdyelacic%2ftuneroom%2f/
permissions/user-04dcfd20-fc73-41d0-a0d8-62d1706e6281" -Method 'DELETE' -
Headers $authHeader
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Event Rules REST API

Endpoint://sites/{siteid/event-rules

Get or create site event rules

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rules

GET Body Sample

```
### GET SITE EVENT RULES ###
GET https://{{host}}/admin/v2/sites/{{Siteid}}/event-rules HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample


```
{"data":[{"type":"eventRule","id":"8d11ec4f-3c6c-4ab9-8045-
fb5c94b38ca0","attributes":{"info":{"Description":"Backup and
Cleanup","Enabled":true,"Folder":"00000000-0000-0000-0000-
000000000000","Name":"Backup and Cleanup","Next":"a220530d-c190-4fa8-
ae4a-
52240f6fee94","Remote":false,"Type":"Timer","apiVersion":"v2","eventRuleV
ersion":"416"},"statements":{"StatementsList":[{"ActionStatement":{"Actio
n":{"CleanupAction":{"DaysToKeepFiles":30,"FileMask":"*.bak","Folder":"C:
\\ProgramData\\Globalscape\\EFT
Server\\Backup","Include":true,"Recursive":false,"TimestampType":"Both"}}
,"IfFailedActions":[]},"ConditionStatement":{"Conditions":[],"ElseAttache
dStatements":[],"IfAttachedStatements":[],"Operator":"Or"},"LoopDatasetSt
atement":{"Params":{"DatasetName":"","EndLoopRow":0,"OrderingColumn":","
```


GET PowerShell Sample

```
### Returns event rule settings ###
### User must obtain the SiteID from Get Sites
Write-Output "ER"
Write-Output "----"
#$siteID = Enter SiteID here
$ERList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rules" -
Method 'GET' -Headers $authHeader
Write-Output $ERList | ConvertTo-Json
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rules

POST Body Sample

```
### CREATE EVENT RULES ###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/event-rules HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
      "type": "eventRule",
      "id": "a220530d-c190-4fa8-ae4a-52240f6fee94",
      "attributes": {
        "info": {
          "Description": "Execute a specified action one time or repeat
```

POST Response Body Sample


```
{"data":{"data":[{"type":"eventRule","id":"c2320fbb-e7cc-4fde-8b41-
ffa655e71e50","attributes":{"info":{"Description":"Execute a specified
action one time or repeat at a specified
interval.","Enabled":true,"Folder":"00000000-0000-0000-0000-
000000000000","Name":"SendToDrobinson","Next":"00000000-0000-0000-0000-
000000000000","Remote":false,"Type":"Timer","apiVersion":"v2","eventRuleV
ersion":"416"},"statements":{"StatementsList":[{"ActionStatement":{"Actio
n":null,"IfFailedActions":[]},"ConditionStatement":{"Conditions":[{"Conte
xtVariable":"","Negate":false,"Operator":"Equals","PropertyID":1000,"Valu
e":{"Flag":false,"Value":"Yes"}}],"ElseAttachedStatements":[],"IfAttached
Statements":[{"ActionStatement":{"Action":{"UploadAction":{"ConnectionPro
fileGUID":"00000000-0000-0000-0000-
000000000000","LocalPath":"C:\\Users\\Administrator\\Desktop\\EFT.exe","R
emotePath":"/%SOURCE.FILE_NAME%","RemoveSource":false,"TransferSettings":
{"Connection":{"CertificateSettings":{"CertId":"00000000-0000-0000-0000-
```


POST PowerShell Sample

```
### CREATE EVENT RULES ###
##POST SITE EVENT RULE settings
Write-Output "Site Event POST"
Write-Output "-----"
$update =

'{
  "data": {
      "type": "eventRule",
      "attributes": {
        "info": {
          "Description": "Execute a specified action one time or repeat at a
specified interval.",
          "Enabled": true,
          "Folder": "00000000-0000-0000-0000-000000000000",
          "Name": "SecondSendToDrobinson",
          "Next": "00000000-0000-0000-0000-000000000000",
          "Remote": false,
```

Endpoint: /sites/{siteid}/event-rules/{ruleid}

Get, create, modify, or delete a specific site event rule

- GET
- POST
- PATCH
- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rules/{ruleid}

GET Body Sample

```
### GET SPECIFIC EVENT RULE ###
@eventRuleID = {{eventRuleList.response.body.$.data[0].id}}
GET https://{{host}}/admin/v2/sites/{{Siteid}}/event-
rules/{{eventRuleID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{"data":{"type":"eventRule","id":"8d11ec4f-3c6c-4ab9-8045-
fb5c94b38ca0","attributes":{"info":{"Description":"Backup and
Cleanup","Enabled":true,"Folder":"00000000-0000-0000-0000-
000000000000","Name":"Backup and Cleanup","Next":"c2320fbb-e7cc-4fde-
8b41-
ffa655e71e50","Remote":false,"Type":"Timer","apiVersion":"v2","eventRuleV
ersion":"416"},"statements":{"StatementsList":[{"ActionStatement":{"Actio
n":{"CleanupAction":{"DaysToKeepFiles":30,"FileMask":"*.bak","Folder":"C:
\\ProgramData\\Globalscape\\EFT
Server\\Backup","Include":true,"Recursive":false,"TimestampType":"Both"}}
,"IfFailedActions":[]},"ConditionStatement":{"Conditions":[],"ElseAttache
dStatements":[],"IfAttachedStatements":[],"Operator":"Or"},"LoopDatasetSt
atement":{"Params":{"DatasetName":"","EndLoopRow":0,"OrderingColumn":"","
```


GET PowerShell Sample

```
### Returns event rule settings ###
### User must obtain the SiteID from Get Sites
Write-Output "ER"
Write-Output "----"
#$siteID = Enter SiteID here
$ERList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rules" -
Method 'GET' -Headers $authHeader
Write-Output $ERList | ConvertTo-Json

$ERID = $ERList.data[0].id

$ERsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-
rules/$ERID" -Method 'GET' -Headers $authHeader
Write-Output $ERsList | ConvertTo-Json
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rules/{ruleid}

POST Body Sample

```
###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/event-rules/2d083578-61de-426f-b357-
96b24d1d45ae HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
{
 "parameters": {
  "operation": "run",
  "parameters": {
   "variables": [
    {
     "name": "On Scheduler (Timer) Event Rule",
     "value": "true"
    }
   ]
  }
 }
}
```

POST Response Body Sample

```
{ "result": { "result": "success", "variables": [ { "name":
"EVENT.DATESTAMP", "value": "20220211" }, { "name":
"EVENT.DATE_TIME_ISO8601", "value": "2022-02-11T22:33:34Z" }, { "name":
"EVENT.EVENTNAME", "value": "On Scheduler (Timer) Event Rule" }, {
"name": "EVENT.NAME", "value": "Scheduler (Timer) Event" }, { "name":
"EVENT.REASON", "value": "Action completed successfully" }, { "name":
"EVENT.TIME", "value": "11 Feb 22 22:33:34" }, { "name":
"EVENT.TIMESTAMP", "value": "223334" }, { "name":
"EVENT.TIMESTAMP_PRECISE", "value": "223334784" }, { "name":
"EVENT.TRANSACTION_ID", "value": "A555F2DC-8B8A-11ec-A822-0022482F4EB1"
}, { "name": "On Scheduler (Timer) Event Rule", "value": "true" }, {
"name": "SERVER.INSTALL_DIRECTORY", "value": "C:\\Program Files
(x86)\\Globalscape\\EFT Server" }, { "name": "SERVER.LOG_LOCATION",
"value": "C:\\ProgramData\\Globalscape\\EFT Server\\Logs\\" }, { "name":
"SERVER.LOG_TYPE", "value": "W3C Extended Log File Format" }, { "name":
"SERVER.NODE_NAME", "value": "DTY2016WinServe" }, { "name":
"SERVER.STATUS", "value": "Yes" }, { "name":
```


POST PowerShell Sample

```
# RPC to execute an event rule

$update =
'{
  "parameters": {
    "operation": "run",
    "parameters": {
      "variables": [
        {
          "name": "On Scheduler (Timer) Event Rule",
          "value": "true"
        }
      ]
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 30
# run an event rule
Write-Output "rpc to run an event rule"
Write-Output "-----"
$folderList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID//event-
rules/2d083578-61de-426f-b357-96b24d1d45ae" -Method 'POST' -Headers
$authHeader -Body $update
Write-Output $folderList | ConvertTo-Json
foreach ($user in $folderList.data)
{
    Write-Output ("User $($user.id): $($user.attributes.loginName)")
}
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rules/{ruleid}

PATCH Body Sample

```
###

PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/event-
rules/{{eventRuleID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data": {
      "type": "eventRule",
      "attributes": {
        "info": {
          "Description": "Execute a specified action one time or repeat
at a specified interval.",
          "Name": "Backups Revisited"
        }
    }
  }
}
```

PATCH Response Body Sample


```
{"data":{"type":"eventRule","id":"8d11ec4f-3c6c-4ab9-8045-
fb5c94b38ca0","attributes":{"info":{"Description":"Execute a specified
action one time or repeat at a specified
interval.","Enabled":true,"Folder":"00000000-0000-0000-0000-
000000000000","Name":"Backups Revisited","Next":"c2320fbb-e7cc-4fde-8b41-
ffa655e71e50","Remote":false,"Type":"Timer","apiVersion":"v2","eventRuleV
ersion":"416"},"statements":{"StatementsList":[{"ActionStatement":{"Actio
n":{"CleanupAction":{"DaysToKeepFiles":30,"FileMask":"*.bak","Folder":"C:
\\ProgramData\\Globalscape\\EFT
Server\\Backup","Include":true,"Recursive":false,"TimestampType":"Both"}}
,"IfFailedActions":[]},"ConditionStatement":{"Conditions":[],"ElseAttache
dStatements":[],"IfAttachedStatements":[],"Operator":"Or"},"LoopDatasetSt
atement":{"Params":{"DatasetName":"","EndLoopRow":0,"OrderingColumn":"","
SortOrder":"Original","StartLoopRow":0,"UseEndLoopRow":false,"UseStartLoo
pRow":false},"Statements":[]},"Type":"Action"},{"ActionStatement":{"Actio
n":{"CleanupAction":{"DaysToKeepFiles":30,"FileMask":"*.*","Folder":"C:\\
ProgramData\\Globalscape\\EFT
Server\\Logs","Include":true,"Recursive":false,"TimestampType":"Both"}},"
IfFailedActions":[]},"ConditionStatement":{"Conditions":[],"ElseAttachedS
tatements":[],"IfAttachedStatements":[],"Operator":"Or"},"LoopDatasetStat
```


PATCH PowerShell Sample

```
##Patch SITE EVENT RULE settings
Write-Output "Site Event Rule PATCH"
Write-Output "-----"
$update =
'{
  "data": {
      "type": "eventRule",
      "attributes": {
        "info": {
          "Description": "Execute a specified action one time or repeat at a
specified interval.",
          "Name": "Backups Revisited"
        }
    }
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-
rules/$ERID" -Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $patchReturn | ConvertTo-Json
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rules/{ruleid}

DELETE Body Sample

```
### GET SPECIFIC EVENT RULE ###
@eventRuleID = {{eventRuleList.response.body.$.data[0].id}}
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/event-
rules/{{eventRuleID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content
Date: Tue, 09 Aug 2022 12:24:53 GMT
Content-Length: 0
Cache-Control: no-cache, no-store, must-revalidate
Expires: -1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
Referrer-Policy: no-referrer
```

DELETE PowerShell Sample

```
$ERID = $ERList.data[1].id

$ERsList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-
rules/$ERID" -Method 'DELETE' -Headers $authHeader
Write-Output $ERsList | ConvertTo-Json
```

Endpoint:/sites/{siteid}/event-rule-folders

Get or create site event-rule-folders

- GET
- POST

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rule-folders

GET Body Sample

```
### GET EVENT RULE FOLDER LIST ###

GET https://{{host}}/admin/v2/sites/{{Siteid}}/event-rule-folders
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
```

GET Response Body Sample


```
{"data":[{"attributes":{"name":"<root>"},"id":"00000000-0000-0000-0000-
000000000000","link":{"self":"/admin/v2/sites/6203305a-d7c6-499e-a59b-
81500765f8f2/event-rule-folders/00000000-0000-0000-0000-
000000000000"},"type":"eventRuleFolder"}],"links":{"self":"/admin/v2/site
s/6203305a-d7c6-499e-a59b-81500765f8f2/event-rule-folders"}}
```


GET PowerShell Sample

```
### Returns all site settings for the specified Site ID ###
### User must obtain the SiteID from Get Sites
Write-Output "ER Folders"
Write-Output "----"
#$siteID = Enter SiteID here
$siteList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-
folders" -Method 'GET' -Headers $authHeader
Write-Output $siteList | ConvertTo-Json
```

Method & URL

POST https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rule-folders

POST Body Sample

```
###
POST https://{{host}}/admin/v2/sites/{{Siteid}}/event-rule-folders
HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}

{
  "data":
    {
      "attributes": {
        "name": "Folder of user events"
      },
      "type": "eventRuleFolder"
    }
}
###
```

POST Response Body Sample

```
{"data":{"attributes":{"isRemote":false,"name":"Folder of user
events"},"id":"38d270a9-6b40-4732-9942-
5bdac9731d93","type":"eventRuleFolder"},"links":{"self":"/admin/v2/sites/
6203305a-d7c6-499e-a59b-81500765f8f2/event-rule-folders/38d270a9-6b40-
4732-9942-5bdac9731d93"}}
```

POST PowerShell Sample

```
##Patch SITE EVENT RULE FOLDER settings
Write-Output "Site Folder PATCH"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes": {
      "isRemote": false,
      "name": "Folder of newer events"
    },
    "type": "eventRuleFolder"
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-
folders/$folderID" -Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $patchReturn | ConvertTo-Json
```

Endpoint:/sites/{siteid}/event-rule-folders/{folderid}

Get, update, or delete a specific site event rule folder data

- GET
- PATCH

- DELETE

Method & URL

GET https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rule-folders/{folderid}

GET Body Sample

```
###
@folderID = {{foldersList.response.body.$.data[0].id}}
GET https://{{host}}/admin/v2/sites/{{Siteid}}/event-rule-
folders/{{folderID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

GET Response Body Sample

```
HTTP/1.1 200 OK Date: Tue, 09 Aug 2022 17:23:43 GMT Content-Type:
application/vnd.api+json ETag: "98C84003" Content-Length: 255 Cache-
Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-
Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy:
no-referrer { "data": { "attributes": { "isRemote": false, "name":
"<root>" }, "id": "00000000-0000-0000-0000-000000000000", "type":
"eventRuleFolder" }, "links": { "self": "/admin/v2/sites/6203305a-d7c6-
```

GET PowerShell Sample

```
Write-Output "ER Folders"
Write-Output "----"
#$siteID = Enter SiteID here
$folderList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-
folders" -Method 'GET' -Headers $authHeader
Write-Output $folderList | ConvertTo-Json

$folderID = $folderList.data[1].id

$foldersList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-
folders/$folderID" -Method 'GET' -Headers $authHeader
Write-Output $foldersList | ConvertTo-Json
```

Method & URL

PATCH https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rule-folders/{folderid}

PATCH Body Sample

```
PATCH https://{{host}}/admin/v2/sites/{{Siteid}}/event-rule-
folders/{{folderID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}


{
  "data": {
    "attributes": {
      "isRemote": false,
      "name": "Folder of new events"
    },
    "type": "eventRuleFolder"
  }
}
###
```

PATCH Response Body Sample

```
HTTP/1.1 200 OK Date: Tue, 09 Aug 2022 18:07:40 GMT Content-Type:
application/vnd.api+json ETag: "1268DCC6" Content-Length: 269 Cache-
Control: no-cache, no-store, must-revalidate Expires: -1 X-Content-Type-
Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy:
default-src 'self' 'unsafe-inline' 'unsafe-eval' data:; Referrer-Policy:
no-referrer { "data": { "attributes": { "isRemote": false, "name":
"Folder of new events" }, "id": "38d270a9-6b40-4732-9942-5bdac9731d93",
"type": "eventRuleFolder" }, "links": { "self":
```

PATCH PowerShell Sample

```
##Patch SITE EVENT RULE FOLDER settings
Write-Output "Site Folder PATCH"
Write-Output "-----"
$update =
'{
  "data": {
    "attributes": {
      "isRemote": false,
      "name": "Folder of newer events"
    },
    "type": "eventRuleFolder"
  }
}'
$update = $update | ConvertFrom-Json
$update = $update | ConvertTo-Json -Depth 10
$patchReturn = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-
folders/$folderID" -Method 'PATCH' -Headers $authHeader -Body $update
Write-Output $patchReturn | ConvertTo-Json
```

Method & URL

DELETE https://[server URL]:[port]/admin/v2/sites/{siteId}/event-rule-folders/{folderid}

DELETE Body Sample

```
###
@folderID = {{foldersList.response.body.$.data[0].id}}
DELETE https://{{host}}/admin/v2/sites/{{Siteid}}/event-rule-
folders/{{folderID}} HTTP/1.1
Authorization: EFTAdminAuthToken {{AuthToken}}
###
```

DELETE Response Body Sample

```
HTTP/1.1 204 No Content Date: Tue, 09 Aug 2022 18:12:00 GMT Content-
Length: 0 Cache-Control: no-cache, no-store, must-revalidate Expires: -1
X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-
Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;
```

DELETE PowerShell Sample

```
$folderID = $folderList.data[1].id

$folderList = Invoke-RestMethod -Uri "$baseURL/v2/sites/$siteID/event-rule-
folders/$folderID" -Method 'DELETE' -Headers $authHeader
Write-Output $folderList | ConvertTo-Json
```

EFT COM API

You can interact directly with EFT from your own custom applications using any COM-enabled programming language such as Visual Basic (VB), Java, or C++. You can create a script with the development IDE of your choice. To create a new script file, you must be familiar with programming concepts and should have experience with COM-enabled programming languages.

The COM API help can be found in the Globalscape online help documentation.

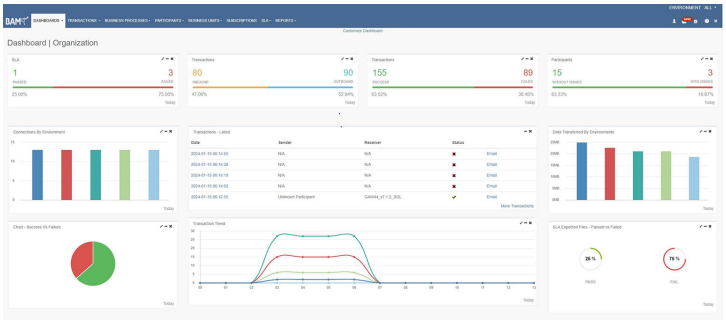
IMPORTANT: The COM API is no longer being updated. Please refer to the REST API documentation, which contains most, if not all, of the COM API features, with more being added in each new version of EFT. You can use the REST API in PowerShell in the Script: PowerShell Action in EFT Event Rules.

Business Activity Monitoring (BAM)

Accolm BAM for Globalscape MFT is a web-based Business Activity Monitoring tool that gives you easy visibility into EFT transactions. This tool is useful for both technical and business users and is used mainly for monitoring business process that have been executed on EFT.

With BAM, you are no longer dependent on administrators and support staff to provide you with information regarding file transfers that your external partners or internal applications have done through the EFT. You can search for transfers and see the statuses of those transfers. This in turn helps you to meet your business-critical Service Level Agreements (SLA).

Refer to http://www.accolm.com/documentation/accolm-bam/for help with installing and using BAM. (The link goes to the Globalscape BAM documentation on the Accolm web site.)



Getting Support

Refer to the topics below for details of getting help.

- Server License Information
- Generate Support Data
- Using the Knowledgebase
- Support Home

Server License Information

When you contact Globalscape Customer Support for assistance, you might be asked to provide your license Information. EFT License Information is displayed in the **About** dialog box. To avoid errors, you can copy and paste the license information into the email that you send to Support. (Personal assistance is available to licensed users that have an existing, unexpired maintenance and support plan.)

You have to be logged in to the server to view or copy the license information, however, you can view the help file or request online support without logging in.

To copy the license information to the clipboard

1. On the main menu, click **Help > About Globalscape EFT**. The **About** dialog box appears.
2. Click anywhere within the **Server License Information** box to select the text, and then click **Copy**. A message appears, stating that the registration information was copied to the clipboard.
3. Click **OK**. You can then paste that information into a text document or email to send to support.

Generate Support Data

If you are working with Globalscape Technical Support on a specific issue with EFT, you can generate a report of key EFT and system data to send to Support. Before sending, be sure to view and, if needed, edit the report.

If the EFT computer does not have Internet access, you can still generate the support data file, and then copy the file onto another computer from which you can upload it to Support's technical portal. If EFT detects that DMZ Gateway is present, it will attempt to use the DMZ Gateway; otherwise, EFT attempts direct connection. You cannot upload the Support data via DMZ Gateway's HTTP proxy.

> **NOTE:** You caninstall the EFT administration interface on another computer that has Internet access, from which you can view and manage EFT, provided that computer can access the EFT computer remotely.

The Generate Support Data wizard automates the process of gathering key EFT and system configuration information to assist with support cases. The ZIP file it generates is saved, by default, at the root of the hard drive on which EFT is installed and is named based on your computer name, such as C:\EFT_WIN-U247V.zip. (You can change this in the Generate Support Data wizard.)

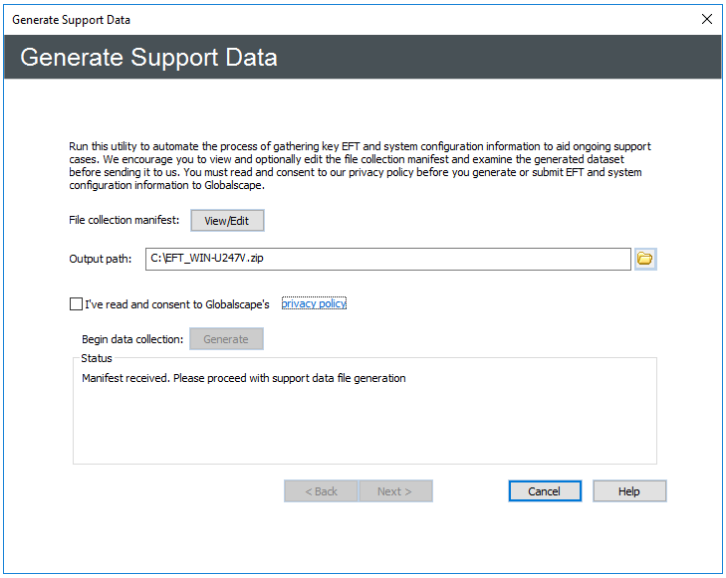
The following data will be collected in the ZIP file in the following folders:

- **Config** - EFT SQLite DB files.
- **Event Logs** - Windows application and system event logs (but ONLY for EFT application)
- **Logs** - EFT log files (going back 1 day, by default)
- **SystemInfo** - system info
- **Advanced Properties json** – EFT configured Advanced Properties (AP)

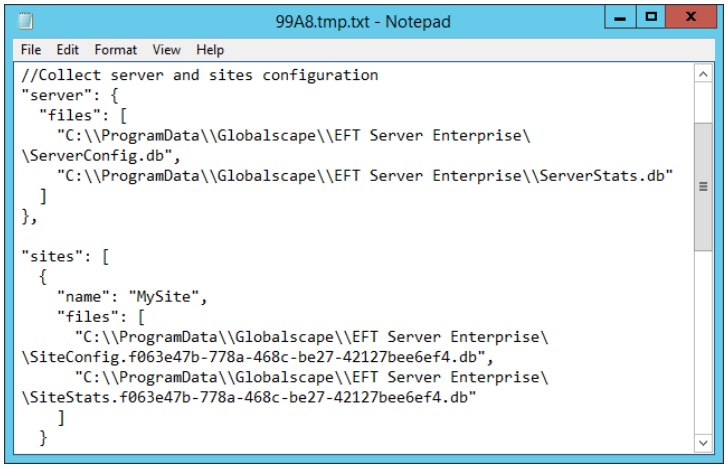
> **NOTE:** You must be logged in to the EFT administration interface to generate support data.

To generate support data

1. On the main menu, click **Help > Generate support data**. The **Generate Support Data** wizard appears.



2. Click **View/Edit**. The file names all of the files and data that will be gathered, including file paths, registry keys, event log items, etc. will appear in an XML file. The file opens in your default TXT reader, such as Notepad.

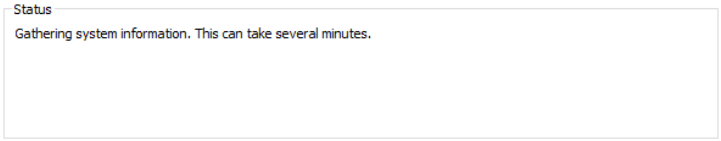


3. This file also determines the number of days to collect data. By default, only 1 day of data is collected. You can edit the file to change the value. For example, to gather more than 1 day's worth of log files, in the text file that you generated, edit the following line:

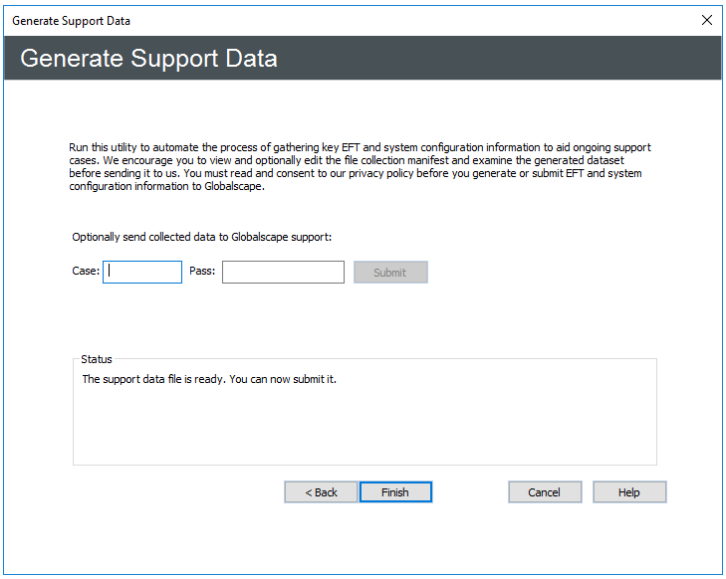
```
//Collect EFT logs for the last 1 day. Change the
        number to collect more logs

"logDays": 1,
```

   And change the value (1) to the number of days data to gather. Be aware that the larger the number, the longer it will take to generate the ZIP file.

4. In **Output path**, specify the default path in which to save the generated dataset. The default is `[root drive]:\EFT_[ComputerName].zip`
5. Click **privacy policy**to open and read the Globalscape Privacy Policyand then select the **I've read and consent to Globalscape's privacy policy** check box.
6. Click **Generate**. (**Generate** is disabled until privacy consent check box is selected.)
7. The **Status** area displays data collection in progress.



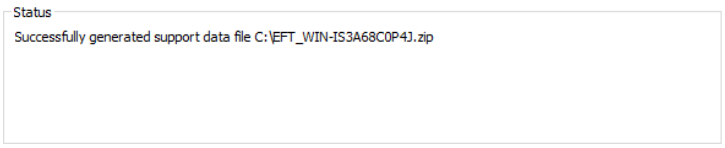
8. Click **Next**.



9. If you were asked to submit the generated file to Support, then provide the case number and the password you were given from Support in the **Case** and **Pass** boxes.
    - If EFT does not have Internet access, you can generate the support data file (saved at the location you specified in the wizard), copy the file onto another computer that does have Internet access, then upload it as requested by Support.
10. **Submit** is disabled until the **Case** and **Pass**boxes are filled. Click **Submit**to send the data.

    If EFT detects that DMZ Gateway is present, it will attempt to use the DMZ Gateway; otherwise, EFT attempts direct connection.

11. A message appears whether connection succeeded or failed. Click **Finish** or click **Back**to try again.



Rest endpoints are also available:

- GET - returns the default template
- GET - returns the bundle generation status
- DELETE - cancels the bundle generation
- POST - Generates telemetry bundle with the specified template
- GET - Returns the list of telemetry bundles

- GET - returns the telemetry bundle
- DELETE - Deletes the telemetry bundle
- /server/telemetry/template
- /server/telemetry/status/{telemetryBundleName}
- /server/telemetry/bundles
- /server/telemetry/bundles/{telemetryBundleName}

Using the Knowledgebase

Globalscape's Knowledgebase (KB), provides various types of articles, such as HOW TO, FAQ, ERRMSG, FIX, and so on. Many articles are created after assisting customers with their specific configuration and troubleshooting issues.

- The **Resources**link provides links to online help and PDFs.
- The **Search**link opens a search utility.
- The **Tags** link list all tags defined on all articles in the KB. You can click a tag to view articles that have been tagged with that keyword. (If there is a keyword that you think should be added to the tags, let us know in the comments of the articles!)

To search the KB

1. Open a web browser and go to https://kb.globalscape.com/
2. On left side in the middle of the page, click **Knowledgebase**. A navigation tree and the latest articles list appear.
3. To view the latest articles just for EFT, click the EFT node.

   The articles are sorted by **Last Modified**date. You can sort the list by Title or Last Modified date by clicking the column header. (With more than 300 articles in the EFT category, searching by title is not usually very efficient. Using the search feature would be more expedient.)
4. To search the KB, click the **Search**link at the top of the page or use the search box at the bottom of the page. When searching, try several different words for the same concept. For example, if you want help with using a script in an Event Rule, search for *command*, *script*, *vb*, *batch*, and so on.

   If the keyword you are using for your search does not find the article you want, but you do eventually find the correct article, please add a comment to let us know that we should add that tag to the article to improve future searches.

Support Home

For the most up-to-date information regarding this version of EFT and its modules; to view version history, updates, and activation instructions; and for other self-help resources, visit the Support Center.