

FORTRA



Globalscape EFT v8.2 Administration Guide

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.

202406250818

Table of Contents

Introduction to EFT Managed File Transfer	24
The EFT Administration Interface	26
Main Menu and Toolbar	28
Server Tab of the Administration Interface	33
Server Tab	33
General Tab of a Server	36
Administration Tab of a Server	37
Security Tab of the Server	39
Logs Tab of a Server	40
SMTP Tab of a Server	41
High Availability Tab of a Server	42
VFS Tab of a Server	44
Status Tab of a Server	45
Report Tab of a Server	47
Site Tabs	48
General Tab of a Site	48
Connections Tab of a Site	49
Security Tab of a Site	50
Web Tab	51
Content Integrity Control Tab	51

Status Bar	52
Administration Interface Session Timeout	52
Closing the Administration Interface	53
Configuring Exit Prompts	55
EFT Web Administration Console	56
Configure EFT to Use Web Admin	56
Logging In to the Web Admin Console	57
Overview	58
User Management	60
View Site and Node Health	66
View Connected Users	67
View Active Automation Rules	67
View Transfers	68
Administrator Account Configuration	69
Account Security Settings Dialog Box	69
Automate Desktop Service Account	70
Active Directory-Based Administration	73
Creating EFT Administrators	73
Administrator Account Permissions	78
Optional Permissions for Administrator	81
Changing an Administrator Password	83
Delegated Administration	84
Enforcing Complex Passwords for Administrator Accounts	86

Enforcing Password History for Administrators	88
Enforcing Password Reset for Administrator Accounts	89
Expiring Administrator Passwords	90
Local Computer Administrators Group	91
Locking Out an Administrator Account	92
Removing Inactive Administrator Accounts	93
Resetting the EFT Administrator Password	95
Specifying Administrator Account's Access Rights	95
Windows Account for the EFT Server Service	96
Creating a Windows User Account for EFT	97
Set Windows NT Permissions for EFT	98
Assigning the Service to a Windows User Account	101
Server Configuration	102
Logging In to Administer EFT	102
Logging Out of EFT in the Administration Interface	103
Starting and Stopping EFT	104
Command-Line Login	105
Listening IP Address and Port	106
Specify the Default Time Stamp	109
Deregister Licenses	109
Administering the Server Service	110
Advanced Properties	112
Email Server Settings	115

Configuring Email Server Settings	115
Create a New Secret for OAuth	120
Create Admin Account for OAuth - Microsoft 365	122
Create a Gmail/ Google Cloud Service Account	126
Extending the Trial	132
Connection Problems	134
Specifying a New Local or Remote EFT	134
New Remote EFT Administration Connection	135
Server Groups	141
Renaming, Deleting, and Moving a Server	142
Monitoring Connections to EFT	144
EFT Messages and Templates	144
File Locations	148
Encryption Algorithms	149
Old Algorithms Removed	149
IPv6 Support in EFT	154
IDN Support in EFT	158
Erasing EFT Configuration	158
Configuring SSL	159
SSL Overview	159
Explicit Versus Implicit SSL	160
SSL Certificates	161
SSL Encryption Algorithms	164

SSL Certificate Compatibility	165
TLS 1.3 Support	167
SSL Certificate Expiration Notification	172
Certificate Chaining	173
Certificate Manager	174
Creating SSL Certificates	175
Enabling SSL on the Server	179
Enabling SSL on the Site	180
TLS Settings on the Site	181
Configuring SSL Authentication for a Settings Template or User Account	182
Exporting a Certificate	183
Exporting a Certificate from PFX to PEM	184
Importing a Certificate	185
SSL Certificate Expiration Notification	186
Signing a Certificate	187
SSL Certificate-Based Login	189
Disabling SSL Connections on the Site	191
Using OpenSSL to Generate/Convert Keys and Certificates	192
Site Configuration	194
How EFT Sites are Defined	194
Creating a Site	195
Creating an Advanced Security Site	214
Propagating an EFT Site	224

Starting or Stopping a Site	229
Protocol Settings	230
FTP/S	232
Allowing Site-to-Site Transfers (FXP)	232
Allowing Client Anti-Timeout Schemes (NOOP)	232
Allowing Multipart Transfers (COMB Command)	233
Allowing the Mode Z Command	235
Configuring FTP or FTPS	235
EFT Support for EBCDIC	237
Encoding for FTP Transfers	237
File Integrity Checking (XCRC)	238
FTP Commands Supported by EFT	240
Specifying a PASV IP or PASV Port Range	240
Specifying the Value Returned by the FTP SYST Command	241
HTTP/S	241
HTTP and HTTPS Overview	242
Configuring HTTP or HTTPS Transfers	245
Customizable HTTP Error Messages	246
Enable HSTS	247
User Access to the Web Transfer Client	248
Online Certificate Status Protocol (OCSP)	249
OCSP Stapling	250
OCSP Stapling in EFT	250

How can I verify that OCSP stapling in EFT is working?	251
Redirecting HTTP to HTTPS	252
EFT Web Service	254
Using Web Service Examples	259
Using WebDAV in EFT	261
SFTP	264
SFTP Outgoing Ciphers and Advanced Properties	264
Outgoing Ciphers	265
SFTP Logging	269
SFTP Encryption Algorithms	270
Enabling SFTP (SSH) on the Server	271
Creating an SSH Key Pair	272
PowerShell Example	275
Available MACs	276
Configuring SFTP for a Site	278
Configuring User SFTP Authentication Options	281
Managing SFTP Keys	283
Encoding for SFTP Transfers	284
Extracting the Public SFTP Key	285
Modifying the SFTP Identification String (Optional)	285
SFTP Key Support	285
SFTP KEX ciphers	288
Specifying SFTP Algorithms	289

SSH Key Formats	289
Using SFTP (SSH) with Radius/RSA SecurID	292
Viewing or Modifying Message Authentication Codes (MAC) Settings	293
AS2	295
Introduction to AS2	295
How EFT Supports AS2	296
Installing and Activating the AS2 Module	299
AS2 Authentication	300
Permutations of Valid Authentication Factors	302
Enabling the AS2 Inbound Listener Service	304
Allowing AS2 Connections to a Site	308
Allowing AS2 Connections in the Settings Template or User Account	308
AS2 Certificates	308
AS2 Account Information Web Page	309
Configuring AS2 Partners	310
Editing AS2 Partner Profiles	310
Configuring AS2 Outbound Partners Using the Wizard	311
Configuring AS2 Inbound Partners Using the Wizard	319
AS2 Inbound Parameters	326
AS2 Outbound (Sender) Parameters	330
Configuring an AS2 Outbound Proxy	335
Initiating AS2 Outbound Transactions	335
Moving Files Received from AS2 Partners	336

Renaming Files Received from AS2 Partners	337
Testing the AS2 Outbound Connection	337
Troubleshooting AS2 Issues	339
AS2 and the Auditing and Reporting Module	340
AS2 Error Warnings and Prompts	341
AS2 Configuration Errors	341
AS2 Transfer Errors	341
Connection Settings	342
Connection Banner Message	342
User Limit Reached Message	345
Quit Session Message	345
Content Integrity Control	346
Content Integrity Control Tab	346
Create a CIC Profile	347
ICAP Options	348
DMZ Gateway Tab - Configuring Perimeter Network Security	351
Enabling DMZ Gateway in EFT	352
Default Network Ports for EFT and DMZ Gateway	354
Automatically Creating a Home Folder for New Users (Site)	357
Azure Data Lake Storage	358
Banning Unwanted File Types	358
Connection Limits Dialog Box	359
Changing a Site's IP Address or Port	360

Controlling Access to the Site by IP Address	363
Changing a Site's Root Folder	366
Configuring Azure Key Vault Support for EFT	367
Configuring the Secrets Module	371
Defining a Connection Profile	375
Deleting a Site	382
Enabling EFS Encryption	383
Enabling the Account Management Page	386
Encryption in EFT	387
Site Encryption	391
Per-Folder Encryption	391
User-Specific Encryption	392
Enabling EFT-Managed Encryption	392
Encryption Algorithms	395
Flooding and Denial of Service Prevention	396
Flood and DoS Prevention Scoring	397
Customizations	400
Internal Domain Settings	401
Specifying External and Internal Domains	404
Workspaces Invitation and Notification Email Links	406
Override VFS Credentials	407
Proxy Protocol	410
Renaming a Site	414

Runtime Template Variables	415
Searching a Site	417
Setting Maximum Concurrent Socket Connections	420
Setting Maximum Concurrent Logins	421
Setting Maximum Connections per User	421
Setting Maximum Connections per IP Address	422
Setting Maximum Transfers per Session	423
Setting Maximum Transfer Size	424
Setting Maximum Transfer Speeds	425
Setting OpenPGP Security for the Site	425
Specifying File Deletion Options	427
Unicode Exceptions	428
Unicode File Transfers	432
Unicode FAQs	433
User Account Details Template	436
User Database Refresh	439
Viewing Site Statistics	440
Viewing Connections to a Site	442
Viewing Transfers To and From a Site	443
Remote Administration	447
Installing the Administration Interface Remotely	447
Remote Administration	449
Remote Administration FAQ	449

Enabling REST API for Remote Administration	452
IP Access Rules for Remote Administration	453
Creating a Remote Connection	456
Configure Remote Administration	461
Starting and Stopping EFT Remotely	462
Remote Administration through DMZ Gateway	463
Introduction to Secure PNC	465
Configuring Secure PNC	465
Configuring Secure PNC using a Self-Signed Certificate	465
Configuring Secure PNC using an EFT Certificate	466
Secure PNC Logging	469
Secure PNC Settings	470
Database Authentication Types	473
Authentication Types	473
Automatically Updating the User Authentication Database	474
Active Directory Authentication	475
Local Security Policy Setting when Using Active Directory Authentication	475
Support for Foreign Groups	478
Removing Domain from the User Folder Name	479
Changing Windows Authentication Options	483
Filter Multiple Active Directory Groups	486
LDAP Authentication	487
Understanding LDAP Authentication	487

Advanced LDAP Filtering	487
Map LDAP Account Attributes to EFT User Account Details	491
Allow AD/LDAP Authentication to EFT through DMZ Gateway	492
Specifying External and Internal Domains	497
Workspaces Invitation and Notification Email Links	499
Map LDAP Users to a Settings Template	500
Connecting to an LDAP Server	501
Changing and Testing LDAP Authentication Options	503
User Home Folders on an LDAP-Authenticated Site	507
Removing Inactive LDAP Accounts from EFT	508
Using Sun Directory LDAP Server	508
ODBC Authentication	508
Using a DSN-Less Connection with ODBC Authentication	508
Changing ODBC Authentication Options	510
Creating Tables for Your ODBC Data Source	511
Script for Creating Necessary ODBC Tables	513
User Home Folders on an ODBC-Authenticated Site	514
Using an ODBC Data Source for User Authentication	514
Establishing a System Data Source Name (DSN)	514
Allow Server to Accept ODBC Database Passwords that are MD5 Hashed	516
Advanced Authentication Modes Module (AAMM)	517
Introduction to the Advanced Authentication Modes Module	517
OpenID Configuration	518

Configuring RSA SecurID Support on an Existing Site	521
RSA SecurID Supported Features	522
RADIUS for User Authentication	523
Configuring RADIUS Support on an Existing Site	525
Enabling or Disabling RSA Authentication via RADIUS	526
SAML (Web SSO) Authentication	527
Introduction to SAML (Web SSO) Authentication	527
Configuring a Site for SAML (Web SSO) Authentication	530
SAML Scope	534
SSO Process	535
Tools for Debugging SAML Communications	536
Validate Username Regex	537
Generate SP Metadata File	538
Web SSO Error Handling	539
Related Knowledgebase Articles	539
Common Access Card Authentication	539
Configuring CAC on an LDAP Site	541
Regulatory Compliance Module	542
Introduction to the Regulatory Compliance Module	542
GDPR Settings	543
GDPR Data Protection Officer	550
GDPR-DPIA Report	551
Personal Data Encryption	553

Privacy Policy	554
Edit the Privacy Policy and Labels	555
Terms of Service Agreement	556
Specify GDPR Status, Privacy Policy Options, and Terms of Service for Users	559
User Account Details Template	561
PCI DSS Compliance	565
Payment Card Industry (PCI) Data Security Standard (DSS)	565
How EFT Addresses PCI DSS Requirements	566
PCI DSS Requirements Addressed	566
PCI DSS Possible Compliance Report Outcomes	574
Warnings for PCI DSS Violations	575
Federal Information Processing Standard (FIPS)	578
FIPS-Certified Library	578
Enabling FIPS Mode for SSL (HTTPS and FTPS) Connections	580
Enabling FIPS for SSH (SFTP) Connections	581
FIPS Mode Event Messages	582
SFTP FIPS	587
EFT Logging and Visibility	591
EFT Client Activity Log	591
EFT Server Log File	598
Domain-Level EFT Server Loggers	599
SFTP Logging	599
SSL/TLS Logging	600

SysLogAppender	601
Installation Logging	601
Viewing Connections to a Site	603
Viewing Server or Node Status	604
Viewing Site Statistics	606
Viewing Transfers To and From a Site	608
Performance Counters	611
Settings Template Tabs	616
How Settings Templates Work	616
Settings Template Tabs	617
General Tab of the Settings Template	617
Connections Tab of the Settings Template	618
Security Tab of the Settings Template	619
Creating or Deleting Settings Templates	619
Inheritance	621
Settings Template Home Folder	621
Enabling or Disabling a Settings Template	622
Moving a User to a Different Settings Template	622
Guest Users Settings Template	623
User Tabs	626
Anonymous User Accounts	626
Banning an IP Address that Uses an Invalid Account	626
User Tabs	628

General Tab of a User Account	629
Connections Tab of a User Account	630
Security Tab of a User Account	631
User Icons	632
Configuring User Account Details	632
Creating a User Account	634
Deleting a User Account	640
Deleting or Disabling Inactive User Accounts	641
Disconnecting Users after a Defined Number of Invalid Commands	642
Disconnecting Users on Timeout	643
Enabling or Disabling a User Account	644
Expiring a User Account	645
Forcibly Logging a User Off of EFT (Kick User)	645
Generating a List of Expired User Accounts and Expiration Dates	646
Managing Multiple User Accounts	649
Specifying Disk Quota	649
Specifying a Home Folder	652
Specifying a User's Permission Group	654
Specifying the Home Folder for AD-Authenticated Users	655
Unlocking a User Account	655
Updating a User Account's Email Address	656
User Account Details Template	657
User Login Credentials Message	660

Username Resend Message	662
Users are Unable to Upload/Download in Home Directory	662
Viewing a User's Home Folder	662
Viewing User Statistics	664
Password Security Settings	665
AD Password Expiration	665
Allowing or Forcing Password Reset	665
Changing a User's Password	668
Disabling or Locking Out an Account	669
Emailing Users' Login Credentials	671
Encrypting Passwords	672
Enforcing Complex Passwords	672
Expiring Passwords	675
Password Reset Messages	677
Prohibiting Password Reuse	679
Reminding Users when Password is About to Expire	681
Controlling Access to Folders (Permission Groups & VFS)	683
Introduction to Permission Groups - Controlling Access to Folders	683
Introduction to the Virtual File System (VFS)	685
How VFS Permissions Work	686
Adding a User or Group to VFS Permissions	689
Adding or Removing Users to or from a Group	691
Creating a New Physical Folder	692

Creating a New Virtual Folder	692
Creating Permission Groups	694
Deleting Groups	695
Deleting a Physical Folder	695
Deleting a Virtual Folder	696
Disabling Inheritance in the VFS	696
Encryption in EFT	697
Site Encryption	702
Per-Folder Encryption	702
User-Specific Encryption	702
Enabling EFT-Managed Encryption	703
Enabling EFS Encryption	705
Mapping a Virtual Folder to a Network Drive	708
Renaming a Group	709
Renaming a Physical Folder	709
Renaming a Virtual Folder	710
Resetting VFS Folder Permissions	711
Setting VFS Permissions	711
Specify Upload Quota in the VFS	712
Viewing Group Membership	715
WTC Users in the VFS	715
Getting Support	716
Generate Support Data	716

Server License Information 719

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 and EFT Arcus.

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.
- **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.
- **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 4880](#) compliant)
- **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.

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.

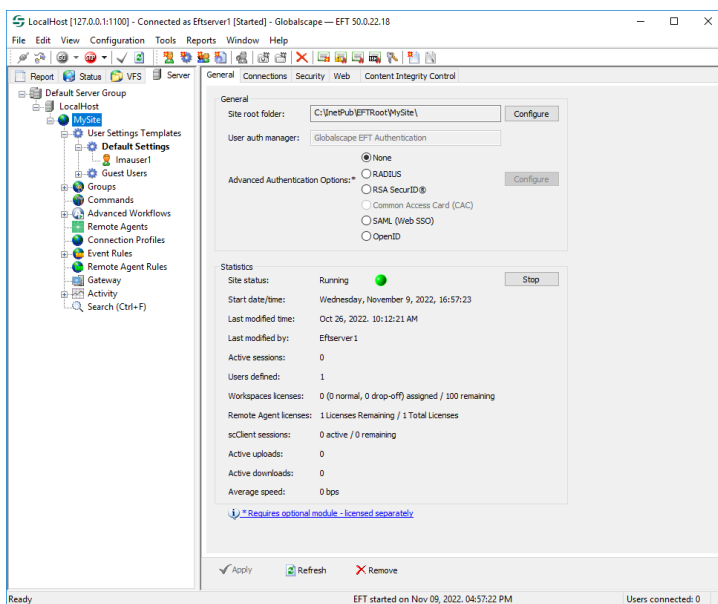
You can login as an administrator using preconfigured accounts created in the internal authentication database, Windows local administrator accounts, or Active Directory-based accounts. A drop-down list is provided from which you can choose **EFT Authentication**, **Currently Logged On User**, or **Windows 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.

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.
	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.

Menu Option	Sub Menu Option	Toolbar	Description
	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.
	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.

Menu Option	Sub Menu Option	Toolbar	Description
	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 .
	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 .
	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)

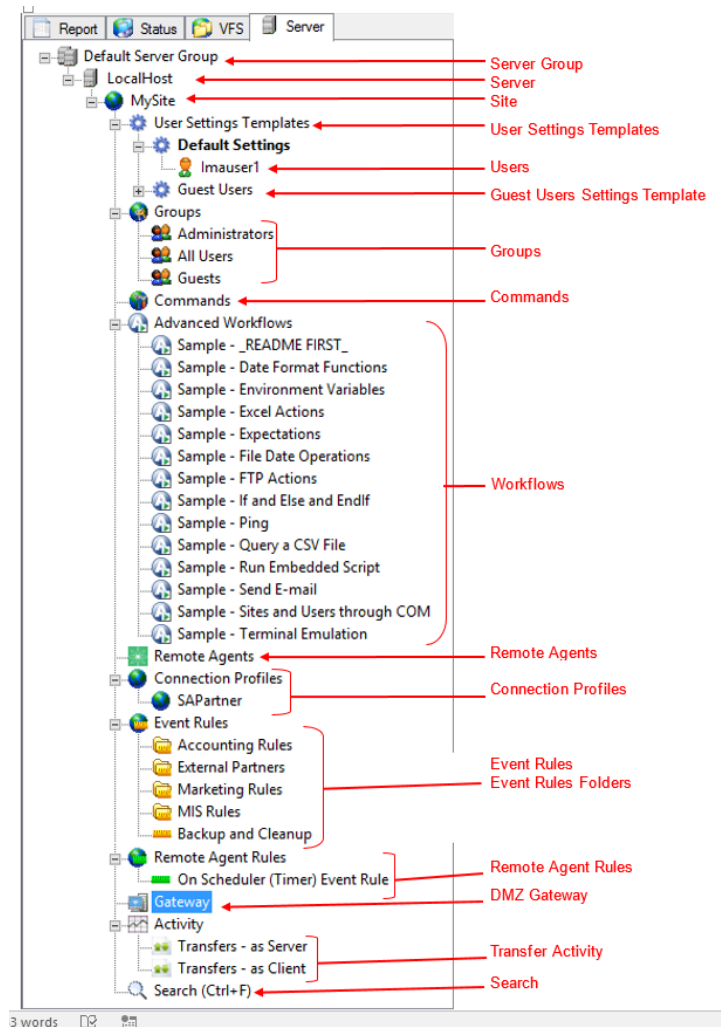
Menu Option	Sub Menu Option	Toolbar	Description
Window	Report	-	Opens the Report tab.
	Status	-	Opens the Status tab.
	VFS	-	Opens the VFS tab.
	Server	-	Opens the Server tab.
Help	Help Contents	-	Opens this Help file.
	Online Knowledge Base	-	Opens the Globalscape Knowledge Base, https://kb.globalscape.com/ .
	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 of the Administration Interface

The topics below describe the Server tab of the EFT administration interface.

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 templates](#) for 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 Site](#) for a specific user, Event Rule, Command, etc.

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 screenshot shows the 'General' tab of the EFT Administration Interface. It features a tabbed interface with 'General', 'Administration', 'Security', 'Logs', 'SMTP', and 'High Availability'. The 'General' tab is active and displays two main sections: 'Statistics' and 'General Settings'.

Statistics

Server status:	Service is started		<button>Stop service</button>
Start date/time:	Mar 01, 2023. 09:01:07 AM		
Uptime:	0 days, 00 hours, 41 minutes		
Last modified time:	Mar 01, 2023. 09:01:07 AM		
Last modified by:	System		
Workspaces licenses:	1 (1 normal, 0 drop-off) assigned / 99 remaining		
Remote Agent licenses:	1 Licenses Remaining / 1 Total Licenses		
Active sessions:	0		
Active uploads:	0		
Active downloads:	0		
Average speed:	0 bps		

General Settings

Server configuration settings:

Default user database refresh interval:

Directory listing date stamp settings:

☐ Use local server time

☒ Use UTC/GMT time

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

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.

The screenshot displays the 'Administration' tab of the EFT Administration Interface. It is divided into two main sections: 'Server Administration Connectivity' and 'Administrator Access and Permissions'.

Server Administration Connectivity:

- Server administrator listening IP:** A text box containing 'All Incoming (IPv4)' with a 'Configure' button next to it.
- Port:** A text box containing '1100'.
- Allow remote administration:** A checkbox that is currently unchecked.
- Enable REST API / web admin:** A checkbox that is currently unchecked.
- REST API / web admin port:** A text box containing '4450'.
- Require SSL for remote administration:** A checkbox that is currently checked, with a 'Configure' button next to it.
- IP ban/access list for remote administration:** A text box with a 'Configure' button next to it.
- Event Rule Change Log:** A section with two radio buttons: 'Off' (selected) and 'On'. Below them is a checkbox for 'Require description' which is unchecked.

Administrator Access and Permissions:

- Admin account names:** A list box containing 'Eftserver1' and 'Local computer\Administrators'. To the right of the list are buttons for 'Add', 'Remove', 'Change Password', 'Account Policy', and 'Password Policy'.
- Selected account permissions policy:** A dropdown menu.
- Optional permissions:** Four checkboxes: 'Run & Edit Reports', 'COM (programmatic control)', 'Manage personal data', and 'Web Admin Client'. All are currently unchecked.
- Assigned to:** A text box with a 'Modify' button next to it.
- Programmatic API Policy:** A checkbox that is currently unchecked, followed by a dropdown menu and a refresh icon.
- Automate Service Account:** A text box with a 'Configure' button next to it.

At the bottom of the interface, there are three buttons: 'Apply' (with a checkmark icon), 'Refresh' (with a circular arrow icon), and 'Remove' (with a red X icon).

- 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.](#)

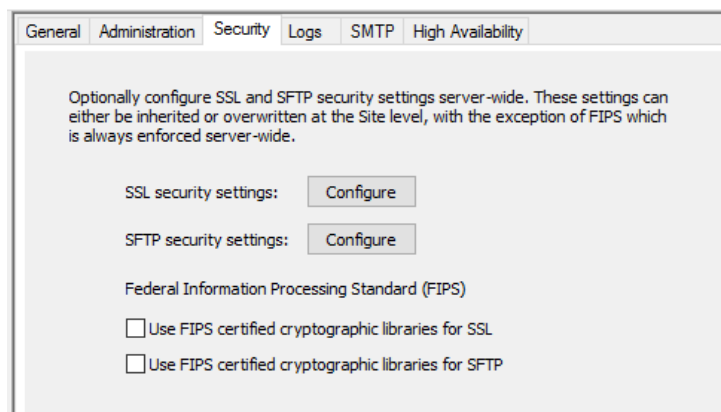
- To add a **Programmatic API Policy**, refer to [Enabling REST API for Remote Admin.](#)

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](#).

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.



The screenshot shows the 'Security' tab selected in the EFT Administration Interface. The tab bar at the top includes 'General', 'Administration', 'Security', 'Logs', 'SMTP', and 'High Availability'. The main content area contains the following text and controls:

Optionally configure SSL and SFTP security settings server-wide. These settings can either be inherited or overwritten at the Site level, with the exception of FIPS which is always enforced server-wide.

SSL security settings:

SFTP security settings:

Federal Information Processing Standard (FIPS)

☐ Use FIPS certified cryptographic libraries for SSL

☐ Use FIPS certified cryptographic libraries for SFTP

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.

The screenshot displays the 'Logs' tab of the EFT Administration Interface. The top navigation bar includes tabs for General, Administration, Security, Logs (selected), SMTP, and High Availability. The main content area is divided into two sections:

Log File Settings

- Folder in which to save log files:
- Log file format: ☒ Encode logs in UTF-8
- Log type:
- Rotate Log File: ☐ Never ☒ Daily ☐ Weekly ☐ Monthly

Audit Database Settings

- ☒ Enable Auditing and Reporting* using ☒ SQL Server ☐ Oracle
- Database host address[\Instance Name]: Database Name:
- or enter DSN or DSN-less connection string and leave the other fields empty.
- Authentication: User: Pass:
- Audit event rule client outbound transfer:
- When a database error occurs:
 - ☐ Stop auditing
 - ☒ Audit to folder:
- ☒ Attempt to reconnect every: seconds
- E-mail notification
 - ☐ On disconnect ☐ On reconnect
 - Recipient list:
- ☒ Refresh statistical fact tables daily
- Connection status: Connected
-

* Requires optional module - licensed separately

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.

General Administration Security Logs **SMTP** High Availability

Specify your server settings for outbound e-mail notifications.

E-mail Server Settings

Authentication: SMTP

SMTP host address: WIN-U247V18I7BA Port: 25

☐ Use Implicit TLS

☐ Enable Authentication

Username:

Password:

From e-mail address: EFT@WIN-U247V18I7BA.com

From name: Globalscape EFT

Send Test Email

Address Book:

Name	Address

Add

Remove

Addresses available in E-mail Notification Event Rule Action

E-mail templates:

- AuthenticationOTPEmail.html.tpl
- AuthenticationOTPEmail.txt.tpl
- CredentialsEmail.tpl
- PasswordResetConfirm.html
- PasswordResetMsg.html
- PasswordResetReminderMsg.html
- PasswordResetUnauthorized.html

Add Edit Remove

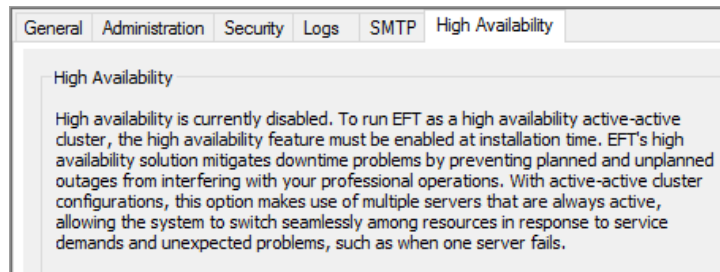
- Click the **Authentication** drop-down box and select **SMTP**, [Gmail OAuth](#), or [Office 365 OAuth](#) for outgoing mail, then refer to [Email Server Settings](#) for details of configuring one of those options for outgoing mail.

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.

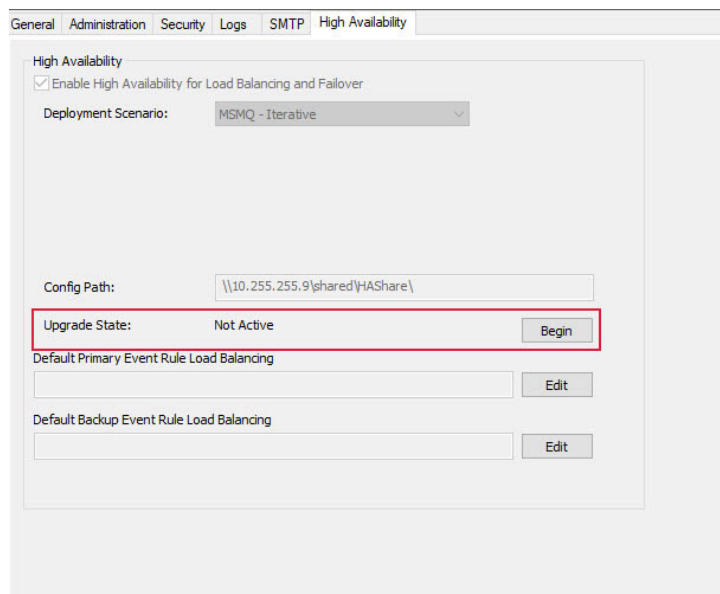
Stand-Alone Server:

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.

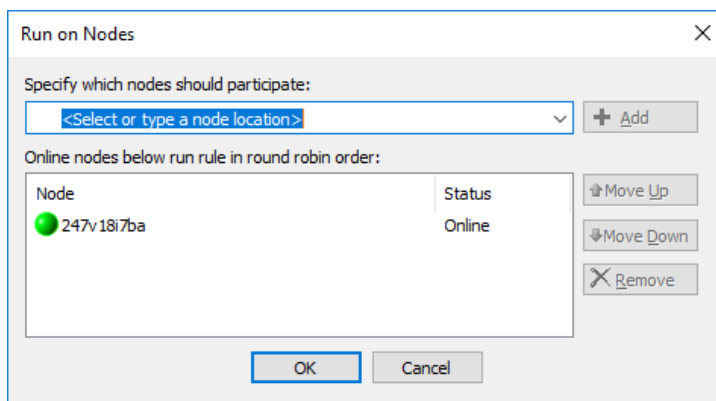
Default Backup Event Rule Load Balancing—Here you can click **Edit** to specify the backup node(s) to run load balanced Event Rules.

- 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.

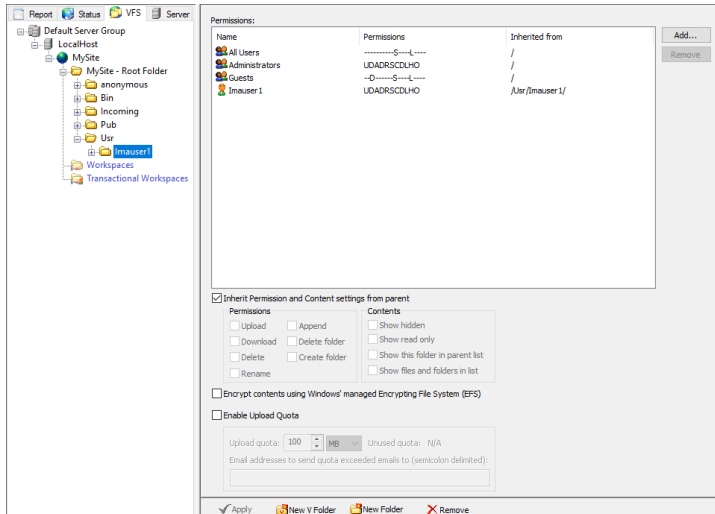
Next to the **Default Primary Event Rule Load Balancing** and **Default Backup Event Rule Load Balancing**, click **Edit**. The **Run on Nodes** dialog box appears.



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

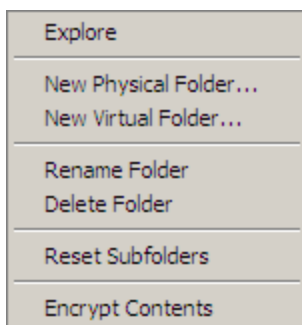
VFS Tab of a Server

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

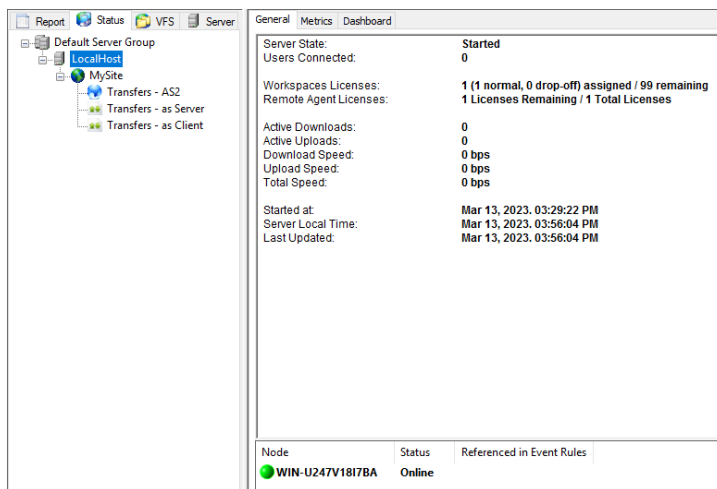
- **Rename Folder** - Allows you to edit the selected folder name
- **Delete Folder** - Deletes the selected folder
- **Reset Subfolders** - Resets permissions on the subfolders of the selected folder
- **Encrypt Contents** - Encrypts the contents of the selected folder (and allows you to specify whether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

Status Tab of a Server

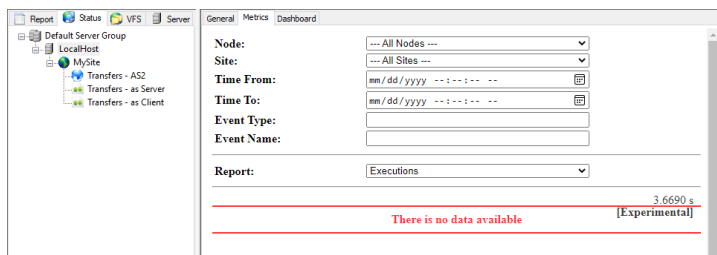
The **Status** tab contains nodes for each Server Group, Server, Site, AS2 transactions, Transfers as Server, Transfers as Client, and each logged-in user.

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.

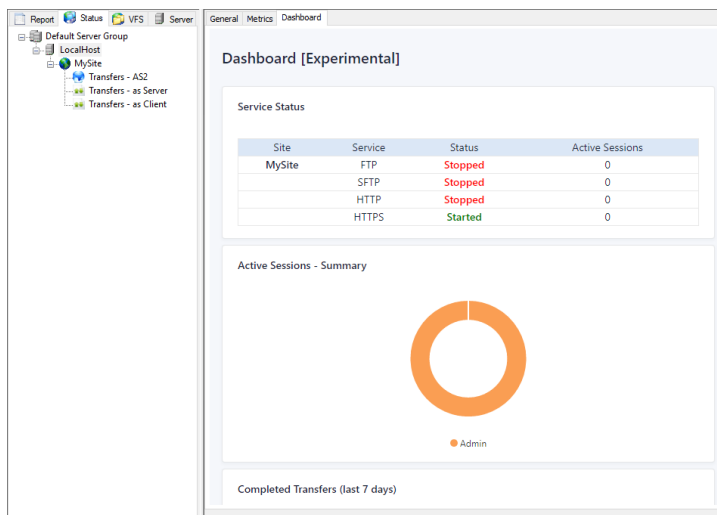
- The **General** tab on the **Server > Status** tab is used to view the status of the selected server, and the status of the node.



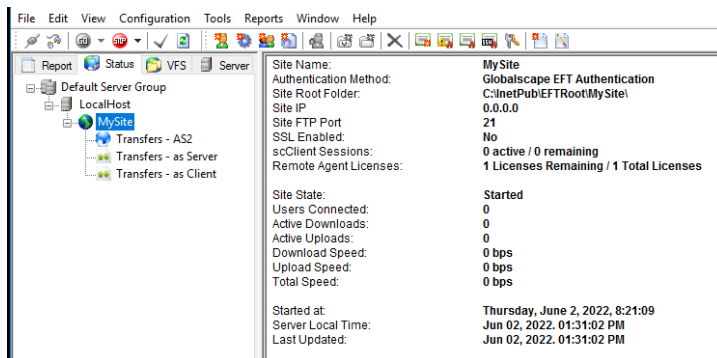
- The **Metrics** tab of the **Server > Status** tab displays metrics from the ARM database. (You must have historical data.)



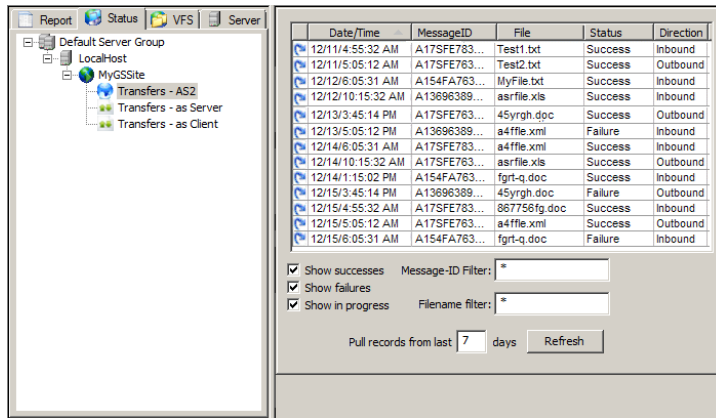
- The **Dashboard** node of the **Server > Status** tab is a visual display of the service status, active status, and completed transfers.



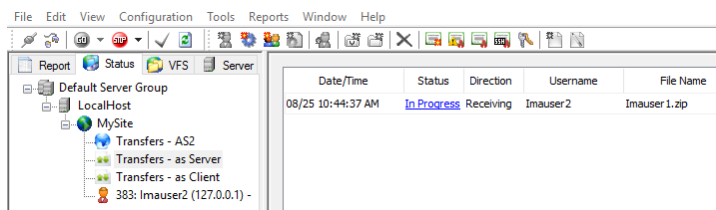
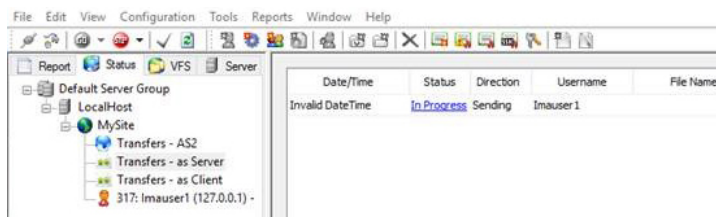
- The **Site** node on the **Status** tab of the administration interface is used to view the status of the Site and logged-in users, including transfers, when EFT was started, number of users connected, and so on. You can also forcibly disconnect FTP/SFTP users from the Site on this tab.



- 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.

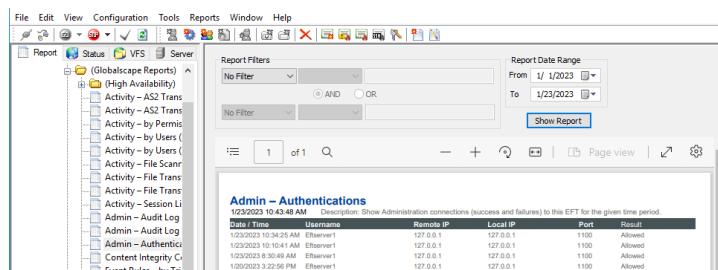


- The **Transfers - as Server** and **Transfers - as Client** nodes are used to view transfers on the Site. (Real-time client transfers require the Auditing and Reporting module.)



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.



Site Tabs

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

The **General** tab is used to change the Site's user authentication settings, view Site statistics, and stop/start the Site.

The screenshot displays the 'General' tab of the EFT Administration Interface for a specific Site. The interface is divided into two main sections: 'General' and 'Statistics'.

General Section:

- Site root folder:** A text box containing the path `C:\inetpub\EFTRoot\MySite` with a 'Configure' button to its right.
- User auth manager:** A dropdown menu showing 'Globalscape EFT Authentication'.
- Advanced Authentication Options:** A group of radio buttons for selecting an authentication method:
 - ☒ None
 - ☐ RADIUS
 - ☐ RSA SecurID®
 - ☐ Common Access Card (CAC)
 - ☐ SAML (Web SSO)
 - ☐ OpenID
 A 'Configure' button is located to the right of these options.

Statistics Section:

- Site status:** Displayed as 'Running' with a green status indicator and a 'Stop' button.
- Start date/time:** Tuesday, October 11, 2022, 14:08:18
- Last modified time:** Oct 10, 2022. 10:16:34 AM
- Last modified by:** Eftserver1
- Active sessions:** 0
- Users defined:** 1
- Workspaces licenses:** 0 (0 normal, 0 drop-off) assigned / 100 remaining
- Remote Agent licenses:** 1 Licenses Remaining / 1 Total Licenses
- scClient sessions:** 0 active / 0 remaining
- Active uploads:** 0
- Active downloads:** 0
- Average speed:** 0 bps

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.

The screenshot displays the 'Connections' tab within the EFT Administration Interface. The interface is organized into several sections:

- General**: Includes tabs for General, Connections (selected), Security, Web, and 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:
 - Protocol selection:
 - ☐ FTP
 - ☐ FTPS (SSL / TLS) - Explicit mode*
 - ☐ FTPS (SSL / TLS) - Implicit mode*
 - ☐ SFTP (SSH2)*
 - ☐ HTTP*
 - ☒ HTTPS (SSL)*
 - ☐ AS2* (with AS2 Config button and notes: - Use yourdomain/as2 for AS2 account management, - Use yourdomain for inbound AS2 transactions)
 - Port configuration:
 - FTP/S Config: 21
 - FTP/S Config: 21
 - FTP/S Config: 990
 - SFTP Config: 22
 - Domain: localhost
 - AS2 Config: 80
 - AS2 Config: 443
 - Require additional factor for HTTP/S auth: *
 - ☒ Allow Globalscape Mobile Transfer Client (MTC) over HTTPS
 - ☐ 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: (Applies to HTTPS, FTPS, Web Services and AS2)
 - SSL security settings:
- Network Usage and Security Settings**:
 - Connection limits:
 - IP access/ban list:
 - Denial of Service settings:

Security Tab of a Site

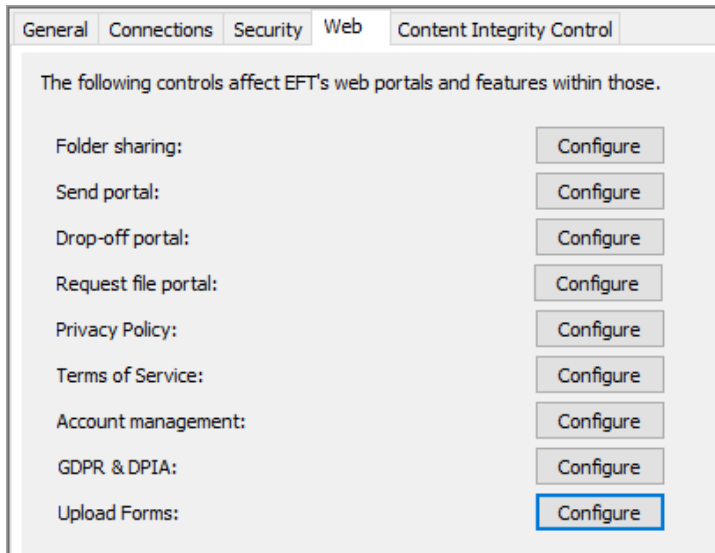
The **Security** tab of the Site node is used to specify password security, account security, and data security settings.

The screenshot shows the 'Security' tab of the EFT Administration Interface. The interface has a top navigation bar with tabs: General, Connections, Security (selected), Web, and Content Integrity Control. The main content area is divided into three sections:

- Password Security:**
 - Invalid login options: [Configure](#)
 - ☐ Enforce strong passwords [Configure](#)
 - ☐ Allow users to reset their passwords
 - ☐ Force new users to change their first-time password immediately upon first use
 - Password expiration options: [Configure](#)
 - ☐ Suppress "Forgot Password" option (LDAP enabled sites only) for: All Domains
 - ☐ Prohibit reuse of previous 4 passwords
 - ☒ Persist username and password credentials for use in Event Rule context variables
 - ☒ Enable option to e-mail users their login credentials
 - ☒ e-mail both username and password together
 - ☐ e-mail the username and password in separate e-mails
 - ☐ e-mail the username only
- Account Security:**
 - ☒ Automatically create a home folder for new users
 - ☒ Grant full permissions to users in their home folder
 - ☐ Disable account after 90 days of inactivity
 - [User Account Details Template...](#)
- Data Security:**
 - Banned file types: [Configure](#)
 - OpenPGP security: * [Configure](#)
 - Secure data removal: * [Configure](#)
 - Encrypted folders: [Configure](#)
 - Secrets module: * [Configure](#)

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.)



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.

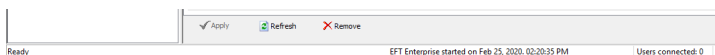
Refer to Global Antivirus Scanning for details of configuring Global antivirus on this tab.

To remove a profile

- To remove a profile, select its name in the list, and then click **Remove**.

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.

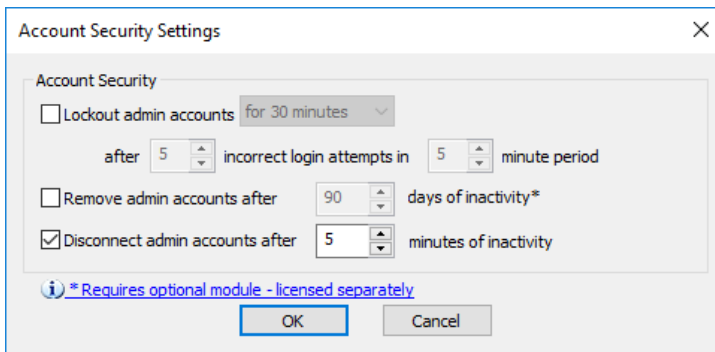
Administration Interface Session Timeout

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 OnMouseClicked) 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. Click **OK** to save the changes.

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.

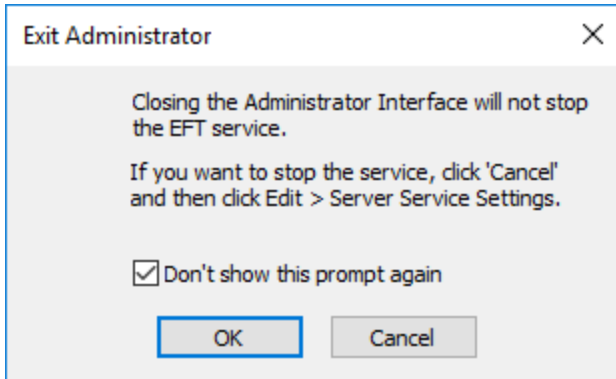
NOTE: If you exit by clicking the server disconnect icon in the upper left corner  , there will not be a prompt; it will just close.

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.



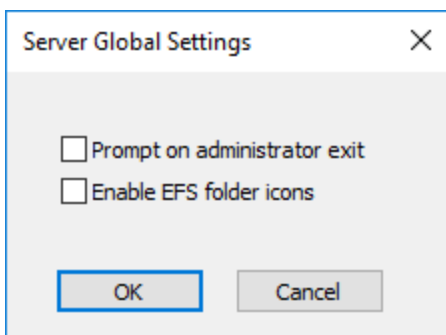
2. If you do not want the **Exit administrator** dialog box to appear when you close the interface, select the **Don't show this prompt again** check box; otherwise, leave it selected.
3. Click **OK**. The administration interface closes.
4. To turn the prompt back on, refer to the procedure below.

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**.

EFT Web Administration Console

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](#)
- [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

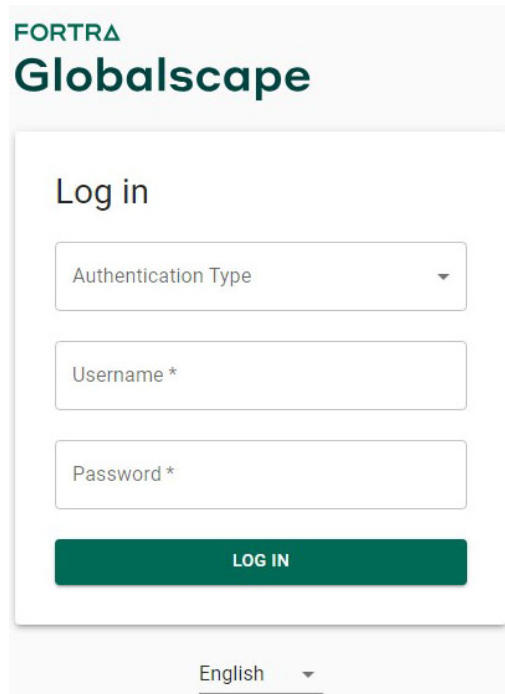
The Web Admin console is based on the REST API, so you must have REST API configured in the EFT administration interface, on the **Server > Administration** tab.

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.



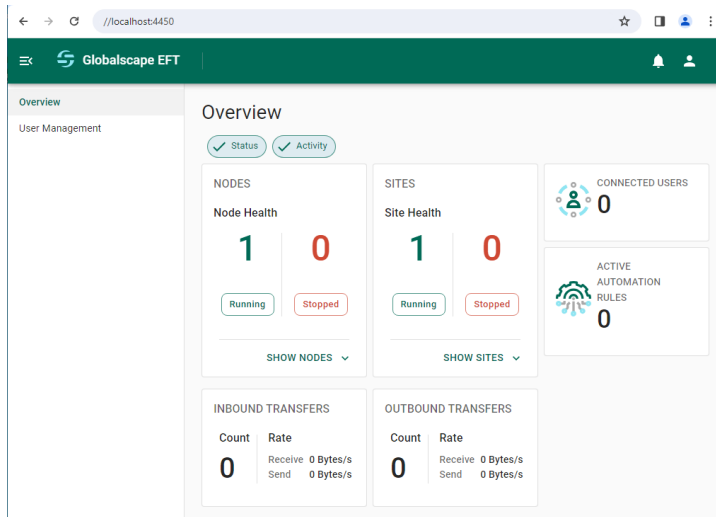
The screenshot shows the Fortra Globalscape Web Admin login page. At the top left is the Fortra logo and the word 'Globalscape'. Below this is a 'Log in' section with a dropdown menu for 'Authentication Type', a text input for 'Username *', and a text input for 'Password *'. A green 'LOG IN' button is positioned below the password field. At the bottom of the page, there is a language selector showing 'English' with a dropdown arrow.

To log in to Web Admin

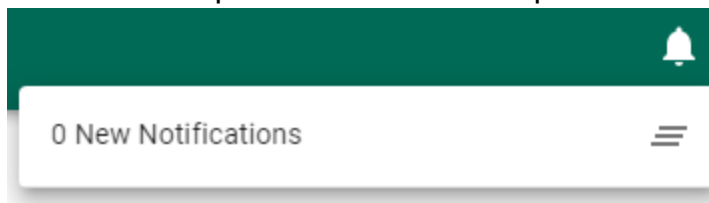
1. Open a browser and go to the *server: port* provided to you by your EFT admin. (For example, on the EFT computer, [https://localhost: 4450](https://localhost:4450).) The **Log In** dialog box appears.
2. Specify your **Authentication type**: EFT Authentication or Active Directory.
3. Provide the username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

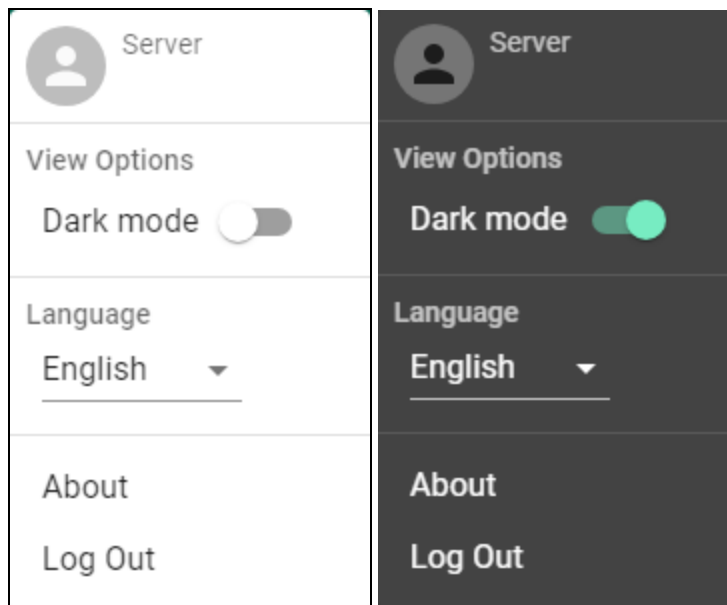


- The **Overview** page displays information about the server and sites that you have configured in EFT, depending on the administrator account type.
 - Server level admin - can see everything
 - Site level admin - nodes widget is gone; you see counts only for resources you have permission to
 - Any 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.

User Management			
FILTER BY			
☐ Username ↑	Email	Template	Groups
☐ Imauser1	kmar@global.com	Default Settings	
☐ Imauser2	imauser2@helpsystems.com	Default Settings	

Rows per page: 15 1-2 of 2

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. 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.)
4. 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.
5. 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.)

Add User to MySite

User Template
Default Settings

Username *

Password *

Email

☐ Email login credentials to this user

ADDITIONAL DETAILS

Home Folder
/Usr/<%USER.LOGIN%>/
Variables: %USER.FULL_NAME%, %USER.LOGIN%, %USER.EMAIL%

☒ Make the home folder the default ROOT folder for this user (recommended)

☒ Grant FULL permissions to this user in their home folder

Group Membership
Users are automatically members of the All Users group

CANCEL ADD USER

Edit User Imauser2

GENERAL DETAILS SECURITY NETWORK USAGE LIMITS

☒ Enabled ☐ Expire on: 07/27/2023

User Template
Default Settings

Home Folder
/Usr/Imauser2/
Variables: %USER.FULL_NAME%, %USER.LOGIN%, %USER.EMAIL%

☒ Make the home folder the default ROOT folder for this user (recommended)

Group Membership
Users are automatically members of the All Users group

CANCEL EDIT USER

Edit User Imauser2

GENERAL

DETAILS

SECURITY

NETWORK USAGE LIMITS

Full Name

Company Name

Description

Email

imauser2@helpsystems.com

DUNS

Phone

Mobile

Pager

Fax

Partner ID

Custom 1

Custom 2

Custom 3

Comments

CANCEL

EDIT USER

Edit User Imauser2

GENERAL

DETAILS

SECURITY

NETWORK USAGE LIMITS

 ☒ Inactivity cleanup

Action

Disable

Days of inactivity

90

User data is subject to GDPR

Unknown

User consent to Privacy Policy (PP)

Unknown

User agreement to Terms of Service (ToS)

Unknown

CANCEL

EDIT USER

Edit User Imauser2

GENERAL DETAILS SECURITY **NETWORK USAGE LIMITS**

☐ Max transfer speed (kbps):

☒ Connection timeout (seconds): 600

☐ Max connections per user:

☐ Max connections from same IP:

☐ Uploads per session:

☐ Downloads per session:

☐ Max upload size (KB):

☐ Max download size (KB):

CANCEL EDIT USER

6. 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.

Delete User

Removing this user and home folder is permanent and cannot be undone.

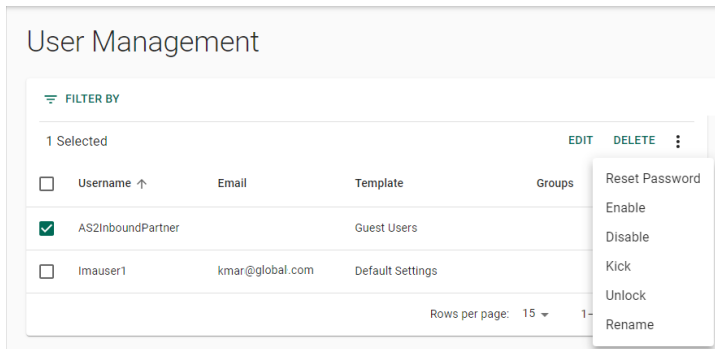
☒ Selected user (Imauser1)

☐ Selected user and their home folder

CANCEL DELETE

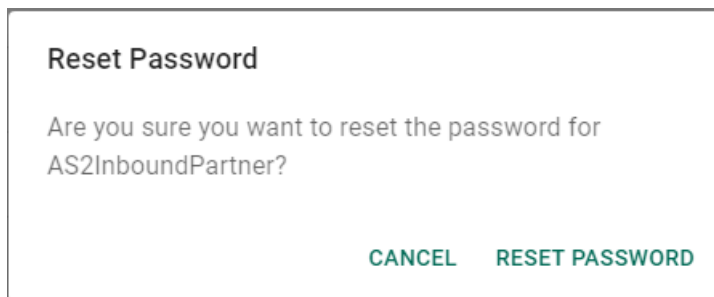
2. Specify whether to delete only the selected user, or the user and their home folder.
3. Click **Delete** to apply.

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



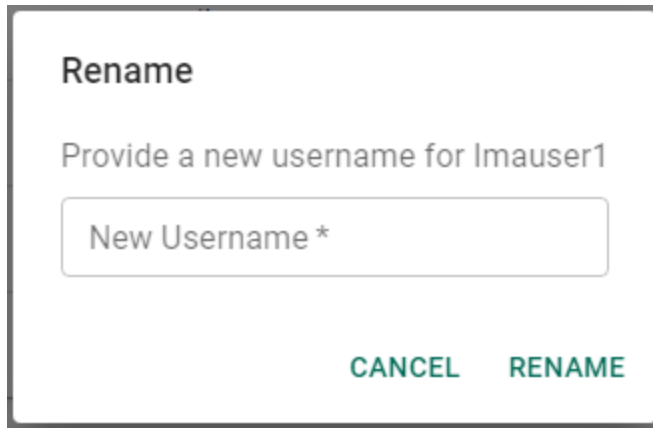
Using this drop-down menu, you can reset the user account password, enable the account, disable the account, kick the user off of EFT, unlock the account, or rename the account.

1. Select the user for whom you want to reset the password.
2. Click the three vertical dots, then click the action that you want to do to the account:
 - a. Reset Password - In the **Reset Password** dialog box, 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.

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



Rename

Provide a new username for lmauser1

New Username *

CANCEL **RENAME**

- c. **Enable** - If an account has become disabled because of expired Workspaces links (for example), click **Enable**.
- d. **Disable** - If an account needs to be disabled (such as an inactive account), you can disable it here.
- e. **Kick** - Use **Kick** if you want to manually disconnect a user from EFT.
- f. **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.

Overview

✓ Status

✓ Activity

NODES

Node Health

1

0

Running

Stopped

SHOW NODES ^

Node	Status
WIN-IS3A68C0	Running

SITES

Site Health

1

0

Running

Stopped

SHOW SITES ^

Site	Status
MySite	Running

View Connected Users

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



CONNECTED USERS

0

View Active Automation Rules

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



ACTIVE
AUTOMATION
RULES

0

View Transfers

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

INBOUND TRANSFERS		OUTBOUND TRANSFERS	
Count	Rate	Count	Rate
0	Receive	0	0 Bytes/s
	Send		0 Bytes/s

Administrator Account Configuration

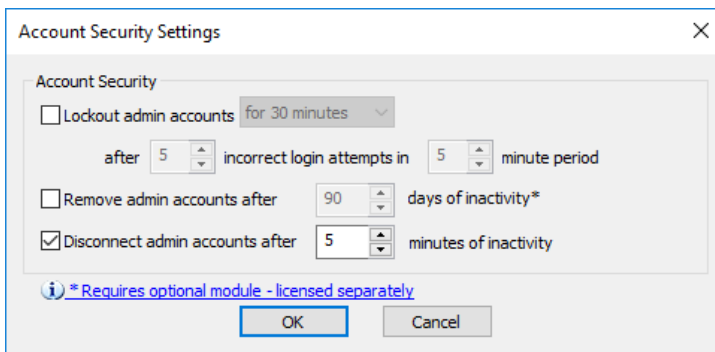
This section describes procedures for creating and managing EFT server administrator accounts.

Account Security Settings Dialog Box

The **Account Security Settings** dialog box is used to [lock out an administrator account](#), [unlock an administrator account](#), and [delete an inactive administrator account](#) automatically, and [change the administration interface session timeout](#) for a specific administrator account.

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 change the default administration interface session timeout](#) for this administrator, select the **Disconnect administrator accounts after** check box, then specify the minutes of inactivity that you need.
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.

Automate Desktop Service Account

The Automate Desktop service 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.

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

NOTE: If no Windows user account is provided and enabled for the Automate service account, EFT Event Rules with Advanced Workflows will not properly execute when the Windows session is locked or logged off. (The EFT event rule will trigger, however, the Automate task will fail.)

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 to prevent the Dialog pop-up from occurring. Tasks will run in the background without popups.

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

NOTE: Do not modify the Automate Desktop 2024 service account in the Microsoft Manage Console **Services** dialog. Only provide the Automate Service Account in the EFT administration interface, as described below, to be used to trigger the workflows when the system is locked or logged off.

To enable the Automate Service Account

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

The screenshot shows the 'Administration' tab of the Administrator Account Configuration dialog. The 'Automate Service Account' section at the bottom is highlighted with a red box. It contains a label 'Automate Service Account:' and a 'Configure' button.

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

The 'Automate Service Account' dialog box is shown. It has a title bar with a close button. Inside, there is a checkbox labeled 'Enable Automate Service Account'. Below it are two text input fields: 'Windows account:' and 'Password:'. A warning message is displayed: 'Warning: Automate Service Account is needed in order to execute Automate tasks via EFT Event Rules when the EFT administrator or EFT service account is logged off the Windows session.' At the bottom are 'OK' and 'Cancel' buttons.

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.

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.

- 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

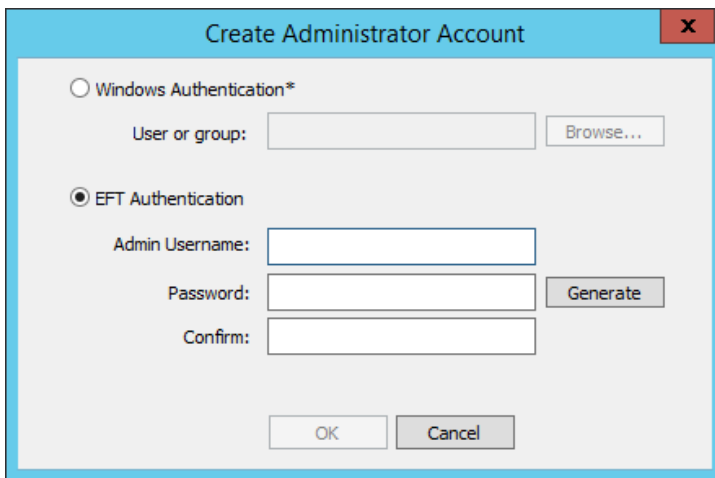
The main EFT administrator account is created when you install EFT. That account can log in and create other administrators with varying permissions. You can give other users and group access to the administrative functions of EFT by creating an administration account for them in the EFT administration 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

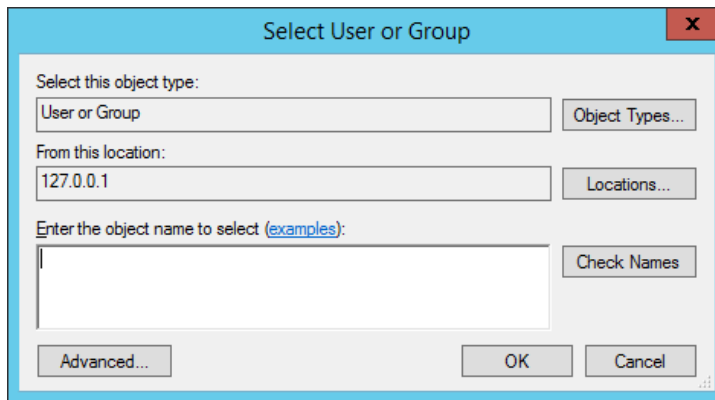
1. In the administration interface, [connect to EFT](#) and click the **Server** tab.
2. On the **Server** tab, click the Server node to which you want to add an administrator account.
3. In the right pane, click the **Administration** tab.
4. In the **Administrator Access and Permissions** area, click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

The image shows a 'Create Administrator Account' dialog box. It has a title bar with a close button (X). Inside, there are two radio buttons: 'Windows Authentication*' and 'EFT Authentication'. The 'EFT Authentication' option is selected. Below 'Windows Authentication*' is a text field labeled 'User or group:' and a 'Browse...' button. Below 'EFT Authentication' are three text fields: 'Admin Username:', 'Password:', and 'Confirm:'. There is a 'Generate' button next to the 'Password:' field. At the bottom are 'OK' and 'Cancel' buttons.

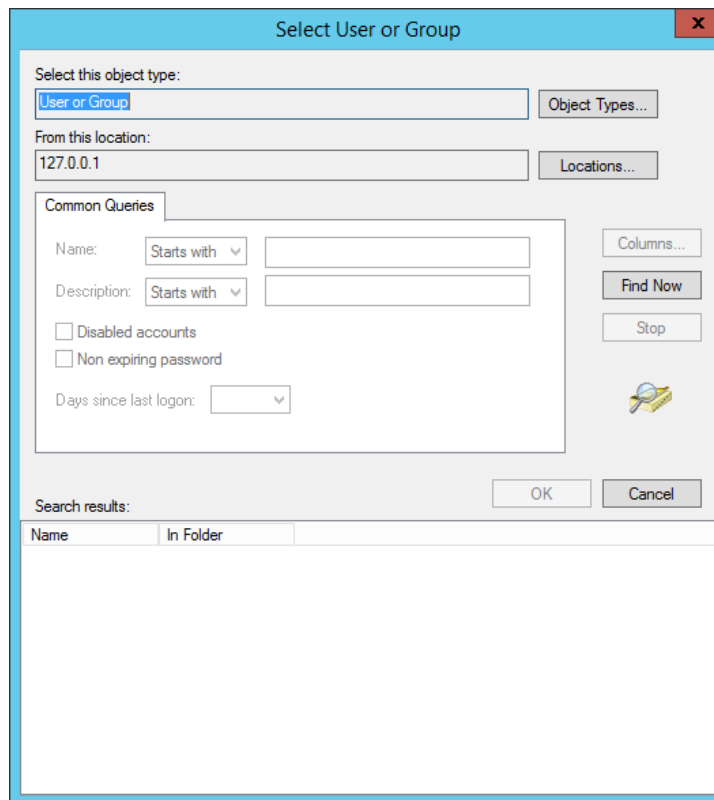
5. Specify either **Windows Authentication** or **EFT Authentication**.
 - If you choose **EFT Authentication**, specify the account details:
 - a. Define a user name for the account.
 - b. Define and confirm a password for the account or click **Generate** to generate a strong password.

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.

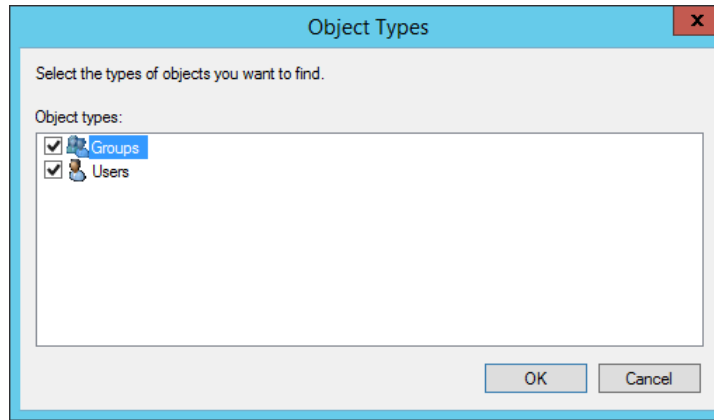
- If you choose **Windows Authentication**, click **Browse** to specify the **User or group**. The **Select User or Group** dialog box appears.



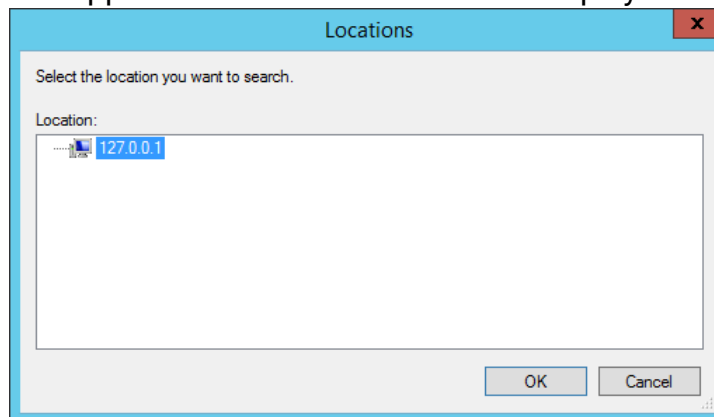
- a. To expand the dialog box, click **Advanced**.



- 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.

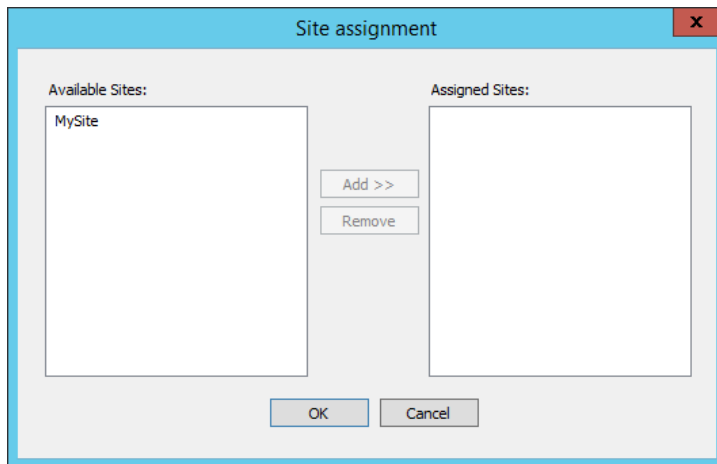


- e. Click a location, and then click **OK**.
- f. In the **Select User or Group** dialog box, use the **Common Queries** area to search for a specific user or group.
- g. After you have specified your search criteria, click **Find Now**. The search results appear.
- h. Click the user or group that you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

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
Delete keys or certificates	Yes	No	Yes, within Event Rules	No	No	No
View Status tab	Yes	Yes	Yes	Yes	No	No

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

Function	Server administrator	Site administrator	Event Rules administrator	Template Settings administrator	User administrator	Change Passwords administrator
View, change users' settings	Yes	Yes, for the assigned Site (s)	No	Yes, for the assigned Settings Template(s)	No	No
Kick and monitor users	Yes	Yes, for the assigned Site (s)	No	Yes, for the assigned Settings Template(s)	No	No
View VFS tab	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
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 screenshot shows the 'Administration' tab with the following sections:

- Server Administration Connectivity:**
 - Server administrator listening IP: All Incoming (IPv4) [Configure] Port: 1100
 - ☐ Allow remote administration
 - ☐ Enable REST API / web admin
 - REST API / web admin port: 4450
 - ☒ Require SSL for remote administration: [Configure]
 - IP ban/access list for remote administration: [Configure]
 - Event Rule Change Log
 - ☒ Off
 - ☐ On
 - ☐ Require description
- Administrator Access and Permissions:**
 - Admin account names:
 - Eftserver1
 - Local computer\Administrators
 - [Add] [Remove]
 - EFT only:
 - [Change Password]
 - [Account Policy]
 - [Password Policy]
 - Selected account permissions policy: [Dropdown]
 - Optional permissions:
 - ☐ Run & Edit Reports
 - ☐ COM (programmatic control)
 - ☐ Manage personal data
 - ☐ Web Admin Client
 - Assigned to: [Text Box] [Modify]
 - ☐ Programmatic API Policy: [Dropdown] [Refresh]
 - Automate Service Account: [Text Box] [Configure]

At the bottom, there are buttons for Apply, Refresh, and Remove.

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](#)).

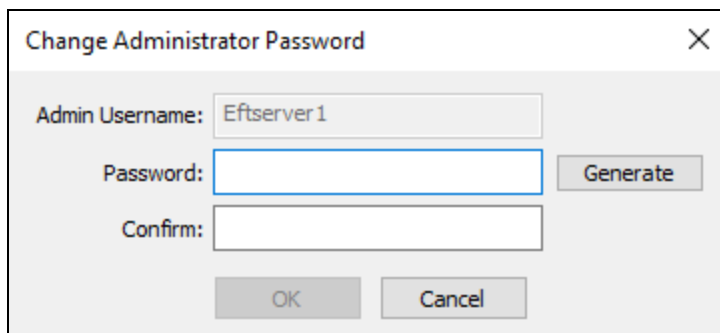
Changing an Administrator Password

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.)



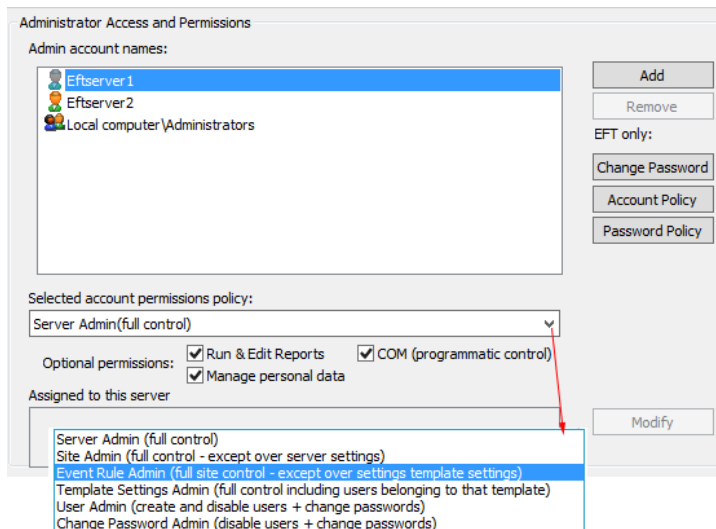
The image shows a dialog box titled "Change Administrator Password" with a close button (X) in the top right corner. Inside the dialog, there are three input fields: "Admin Username:" with the value "Eftserver1", "Password:" (empty), and "Confirm:" (empty). To the right of the "Password:" field is a "Generate" button. At the bottom of the dialog are "OK" and "Cancel" buttons.

Passwords are case-sensitive.

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 accounts](#) that 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.

List users for settings template: All available

Name	Status	Expires	Site
jbug	Enabled	Never	GSAuth
anonymous	Enabled	Never	Paris
bboop	Enabled	Never	San Diego
bob	Enabled	Never	Paris
dbeckham	Enabled	Never	London
dduck	Enabled	Never	San Diego
bpitt	Enabled	Never	San Diego
gclooney	Enabled	Never	San Diego
dknotts	Enabled	Never	San Diego
gdepardieu	Enabled	Never	Paris
mgenobli	Enabled	Never	San Antonio

☒ Enabled

Change password

Unlock

Create New User

- **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.

List users for settings template: All available

Name	Status	Expires	Site
jbug	Enabled	Never	GSAuth
anonymous	Enabled	Never	Paris
bboop	Enabled	Never	San Diego
bob	Enabled	Never	Paris
dbeckham	Enabled	Never	London
dduck	Enabled	Never	San Diego
bpitt	Enabled	Never	San Diego
gclooney	Enabled	Never	San Diego
dknotts	Enabled	Never	San Diego
gdepardieu	Enabled	Never	Paris
mgenobli	Enabled	Never	San Antonio

☒ Enabled

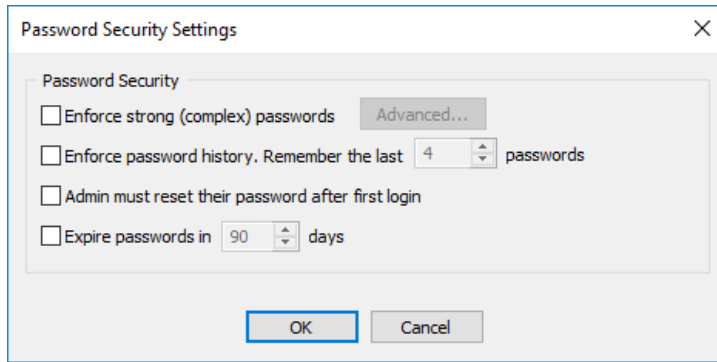
Change password

Enforcing Complex Passwords for Administrator Accounts

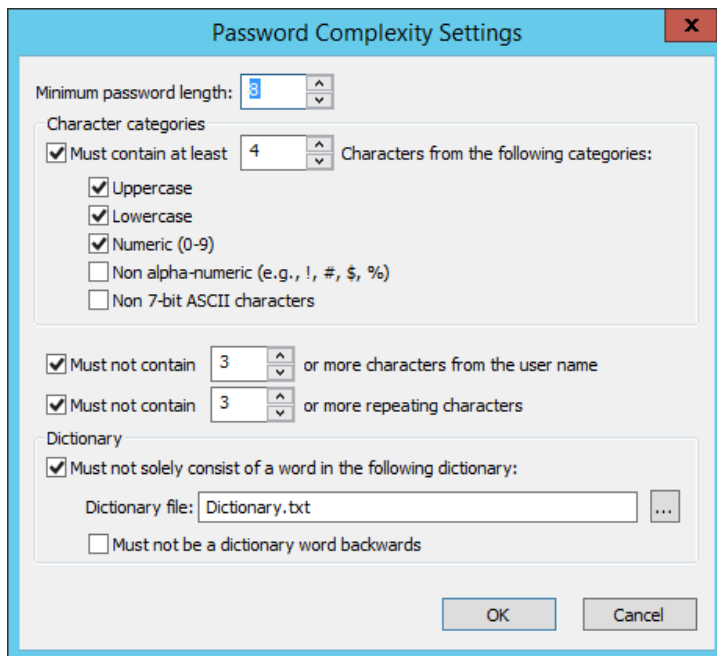
When you create or edit EFT-managed administrator accounts, you can specify that all administrator accounts be required to adhere to certain password complexity rules.

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 default is 8 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	8	6 - 99
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.

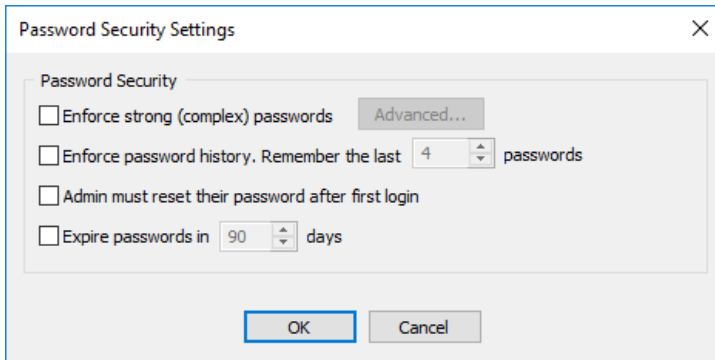
Enforcing Password History for Administrators

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.

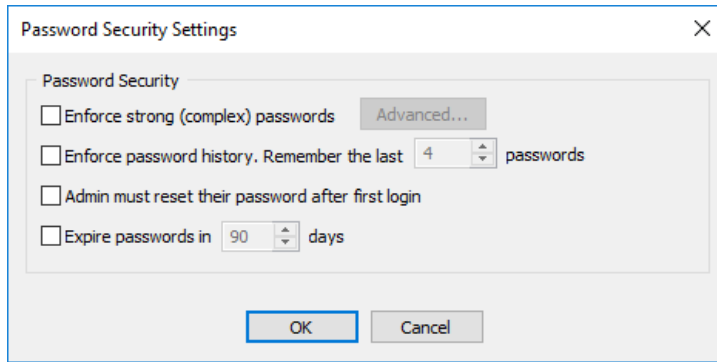
Enforcing Password Reset for Administrator Accounts

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.

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.

Expiring Administrator Passwords

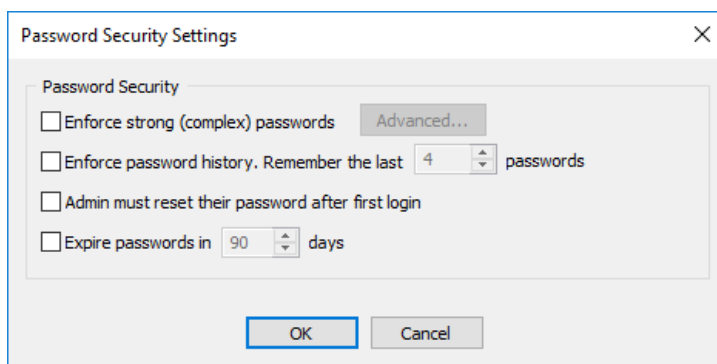
If **Expire Passwords** is enabled and a user logs in with an administrator account with a temporary password, EFT prompts the user to supply a new password. Each day it also checks whether passwords are <n> days from expiration, and those passwords are flagged for reminders, if reminders are enabled.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

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.

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.

Administrator Access and Permissions

Admin account names:

- Eftserver1
- Local computer\Administrators

Buttons: Add, Remove

EFT only:

Change Password

Account Policy

Password Policy

Selected account permissions policy:

Server Admin(full control)

Optional permissions:

- ☒ Run & Edit Reports
- ☒ COM (programmatic control)
- ☒ Manage personal data

Assigned to this server

Modify

☒ REST administrator role: Server Admin(full control)

- 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

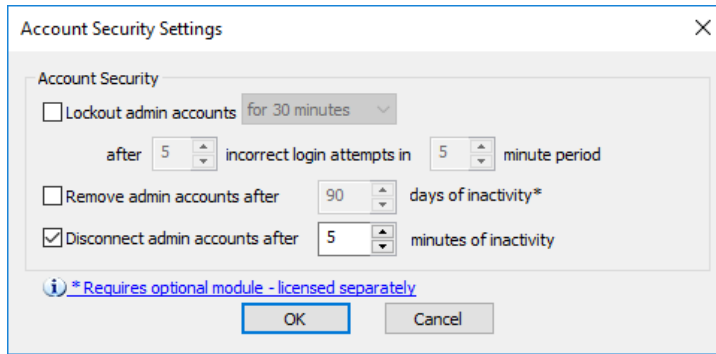
EFT can automatically lock out an administrator account after a specified number of incorrect login attempts over a specified time.

On a high security-enabled Site, if you clear the **Lockout** check box, increase the number of incorrect login attempts to more than 6 or set the attempt period to more than 5 minutes, a warning message appears.

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.
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.
7. To resume account security, click **Account Policy**. The **Administrator Account Security** dialog box appears.
8. Select the **Lockout** check box.
9. Click **OK** to close the dialog box.
10. Click **Apply** to save the changes.

Removing Inactive Administrator Accounts

EFT allows you to disable or remove user accounts; however, *administrator* accounts can only be removed, not disabled.

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.

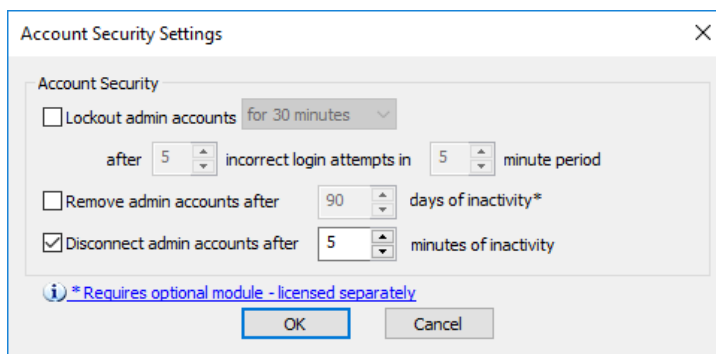
If a user attempts to log in remotely to EFT with an administrator username that does not exist or an incorrect password, a warning message appears in the administration interface.

To 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 Password](#) instead 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.

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.

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.

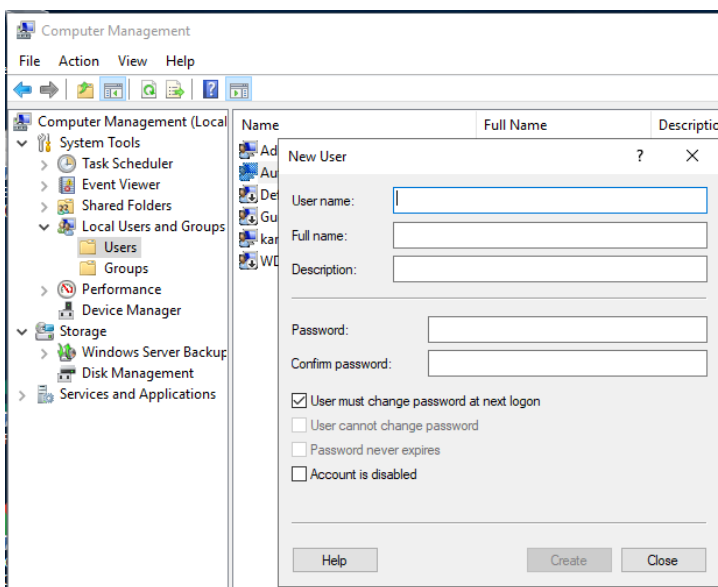
Refer to [Local Security Policy Setting when Using Active Directory Authentication](#) for more information about configuring EFT on an AD network. Consult with your AD network administrator for assistance, if necessary.

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.

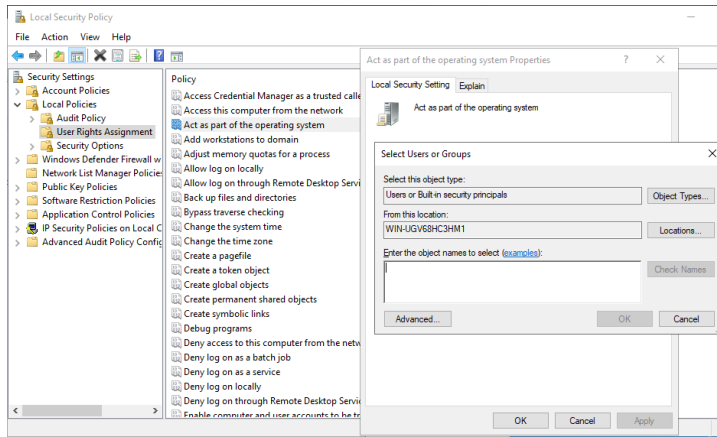
Creating a Windows User Account for EFT

To create a user account in Windows

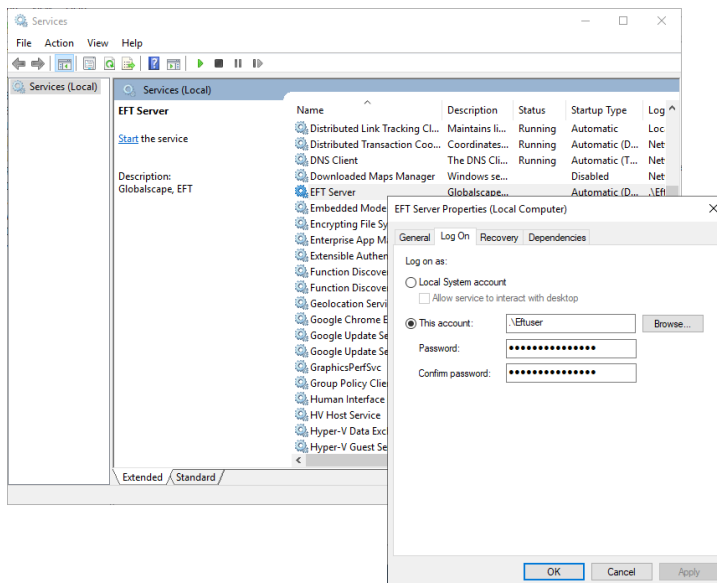
1. After you install EFT, open the Computer Management console. (In the Windows **Search** box, type `computer management`.)
2. Expand the **Local users and Groups** node, right-click **Users**, then click **New User**. The **New User** dialog box appears.



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.

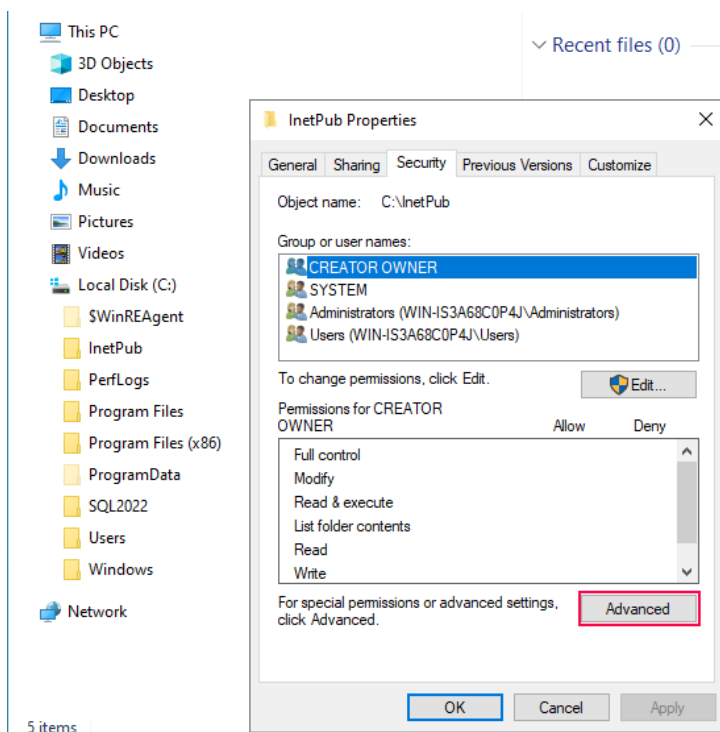
In addition to the individual permissions, Windows NT permissions also provide access levels that are pre-built sets of the existing permissions. Typically, you assign an access level to a user rather than granting individual permissions. One such access level is called "No Access," which does not contain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

To view and edit the permissions for a folder or file

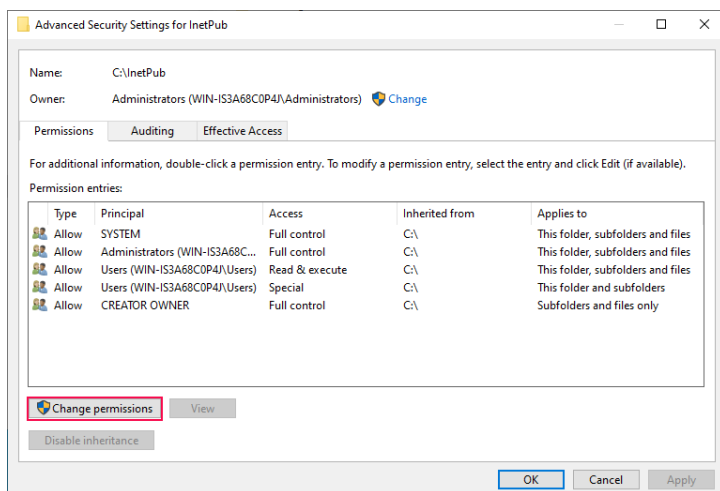
1. In Windows File Explorer, right-click the file or folder, then click **Properties**.
2. On the **Security** tab, click **Permissions**. The appearance of this dialog box is slightly different for files and directories and for different versions of Windows (W2K, XP, etc.).

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

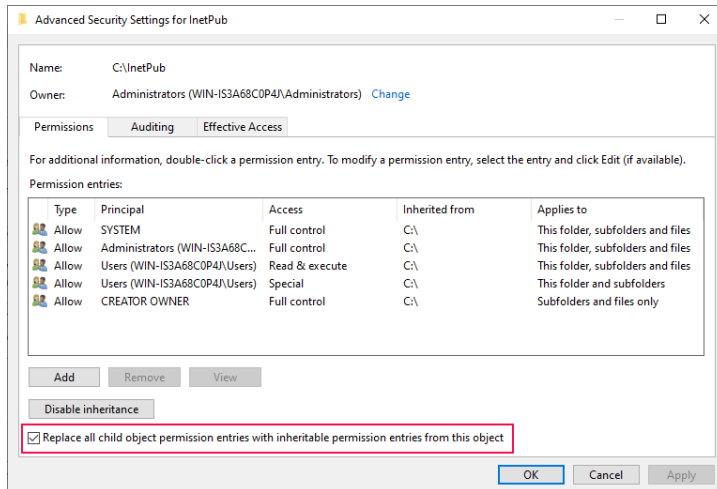
1. In Windows File Explorer, right-click the EFT user home folders directory (for example, C:\InetPub\), then click **Properties**.



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.



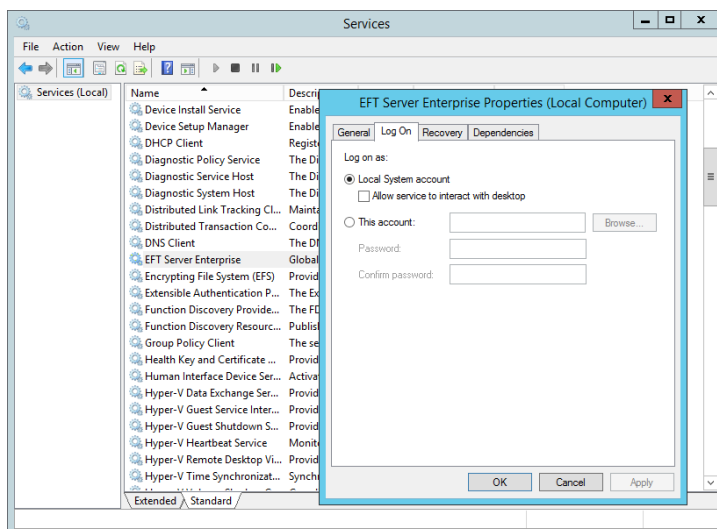
- At the bottom of this tab, select the **Replace all child object permissions entries with inheritable permission entries from this object** check box. This will ensure that child objects will inherit the permissions of the selected object.

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

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



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

Server Configuration

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

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 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.

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

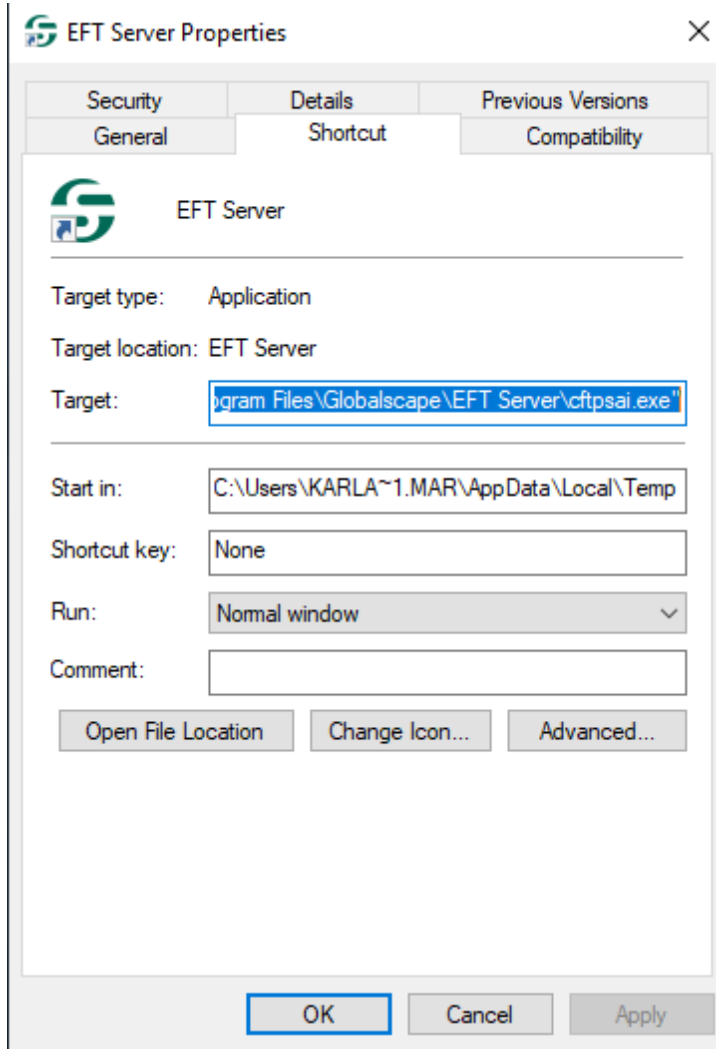
1. Open a command prompt (**Start > Run > cmd**).
2. Change to the directory in which EFT is installed (for example, **cd C:\Program Files\Globalscape\EFT Server**).
3. Type the name of the administration interface executable (**cftpsai.exe**), followed by the administrator listening IP address and port, 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 Setup](#) wizard. 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.

The screenshot shows the EFT Administration interface with the **Administration** tab selected. The interface is divided into two main sections: **Server Administration Connectivity** and **Administrator Access and Permissions**.

Server Administration Connectivity:

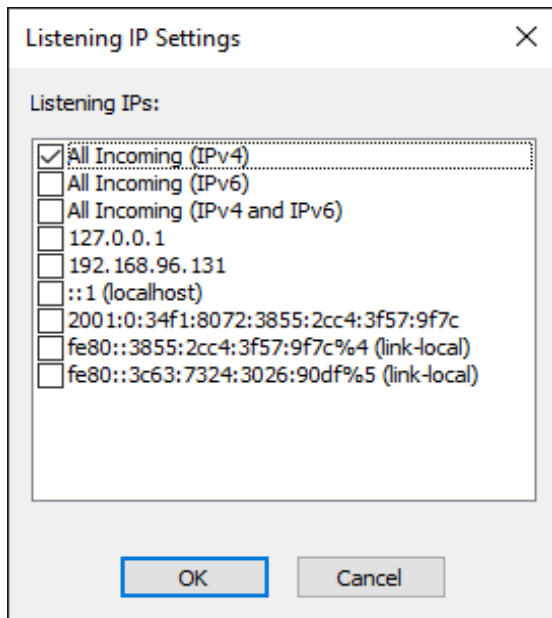
- Server administrator listening IP:** A dropdown menu showing "All Incoming (IPv4)". A **Configure** button is next to it.
- Port:** A text box containing "1100".
- ☐ **Allow remote administration**
- ☐ **Enable REST API / web admin**
- REST API / web admin port:** A text box containing "4450".
- ☒ **Require SSL for remote administration:** A **Configure** button is next to it.
- IP ban/access list for remote administration:** A **Configure** button is next to it.
- Event Rule Change Log:**
 - ☒ **Off**
 - ☐ **On**
 - ☐ **Require description**

Administrator Access and Permissions:

- Admin account names:** A list box containing "Eftserver1" and "Local computer\Administrators".
 - Add** button
 - Remove** button
 - EFT only:**
 - Change Password** button
 - Account Policy** button
 - Password Policy** button
- Selected account permissions policy:** A dropdown menu.
- Optional permissions:**
 - ☐ **Run & Edit Reports**
 - ☐ **COM (programmatic control)**
 - ☐ **Manage personal data**
 - ☐ **Web Admin Client**
- Assigned to:** A text box.
- Modify** button
- ☐ **Programmatic API Policy:** A dropdown menu.
- Automate Service Account:** A **Configure** button.

At the bottom of the interface, there are three buttons: **Apply** (with a checkmark icon), **Refresh** (with a circular arrow icon), and **Remove** (with a red X icon).

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

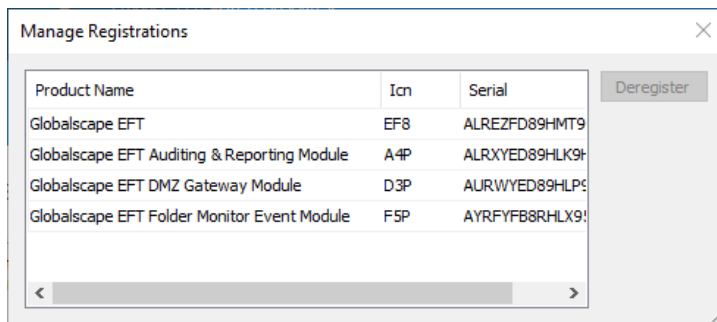
There are a variety of reasons why you might want to "deregister" the server and/or modules licenses, such as:

- 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**.

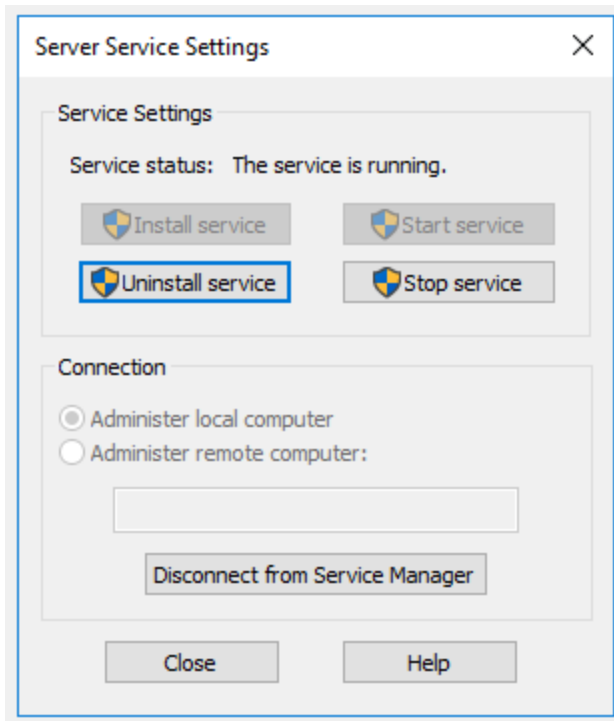
The dialog box refreshes and the selected product is removed from the list. The license is now available to register on another server.

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**.

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.

```
{
"AuditSuccessSocketConnections": "true",
"AuditIsInterl": "true",
"SAMLSSODigestAlgo": "sha256"
}
```

(See an example in the procedure below. Refer to <https://tools.ietf.org/html/rfc8259#section-3> for 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.

EFT doesn't validate the JSON file itself for acceptable or unacceptable names and values. It only reads names and validates their values.

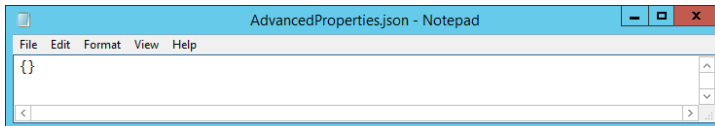
If the "value" is wrong or malformed, the EFT server service will not start, and an error is written to the log.

If the Advanced Property name is misspelled, it is ignored, but the service will start. That is, if EFT was expecting "EncryptPersonalData" but you spelled it "EncryptPersonelData" EFT will ignore it.

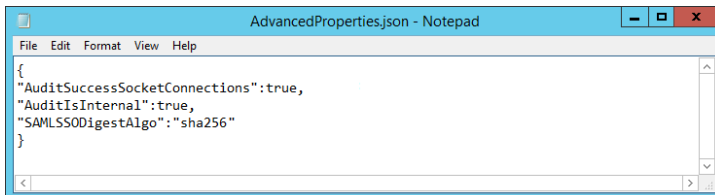
To edit or view the Advanced Properties file

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. (See screenshot above.)
 - c. For multiple objects, add a comma after the value, then add a new line and type the second object.
 - 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.

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 [Events](#) occur, 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.

Configuring 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 [Events](#) occur, 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**.

General Administration Security Logs SMTP High Availability

Specify your server settings for outbound e-mail notifications.

E-mail Server Settings

Authentication: SMTP

SMTP host address: WIN-U247V1817BA Port: 25

☐ Use Implicit TLS

☐ Enable Authentication

Username:

Password:

From e-mail address: EFT@WIN-U247V1817BA.com

From name: Globalscape EFT

Send Test Email

Address Book:

Name	Address

Add

Remove

Addresses available in E-mail Notification Event Rule Action

E-mail templates:

- AuthenticationOTPEmail.html.tpl
- AuthenticationOTPEmail.txt.tpl
- CredentialsEmail.tpl
- PasswordResetConfirm.html
- PasswordResetMsg.html
- PasswordResetReminderMsg.html
- PasswordResetUnauthorized.html

Add Edit Remove

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](#).

General Administration Security Logs SMTP High Availability

Specify your server settings for outbound e-mail notifications.

E-mail Server Settings

Authentication: GMail OAuth

Service account credentials:

Project ID:

Private key ID:

Client email:

Gmail Account:

From e-mail address: EFT@WIN-U247V18I7BA.com

From name: Globalscape EFT

- 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 Account for OAuth - Microsoft 365](#).

General Administration Security Logs SMTP High Availability

Specify your server settings for outbound e-mail notifications.

E-mail Server Settings

Authentication: Microsoft 365 OAuth

Microsoft 365:

Client ID:

Client Secret:

Tenant ID:

From e-mail address: EFT@WIN-U247V18I7BA.com

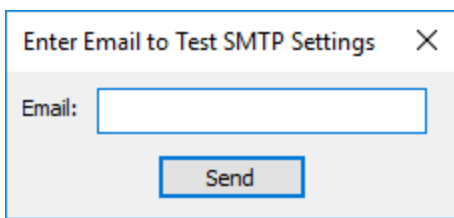
From name: Globalscape EFT

- **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.

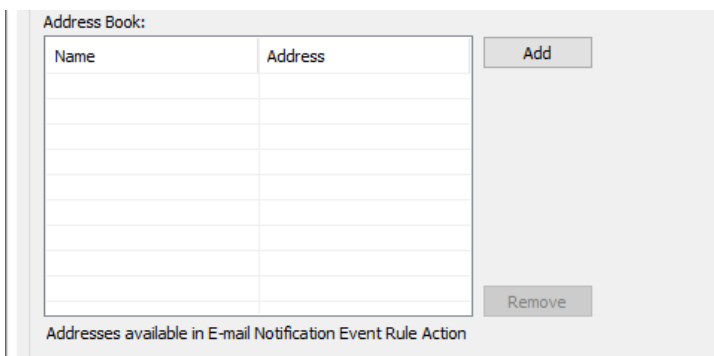
NOTE: Microsoft recommends that you disable SMTP AUTH organization-wide or per mailbox (hosted Microsoft 365). For more details, refer to the Microsoft topic at <https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission>.)

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.



The dialog box titled "Enter Email to Test SMTP Settings" has a close button (X) in the top right corner. It contains a label "Email:" followed by a text input field. Below the input field is a button labeled "Send".

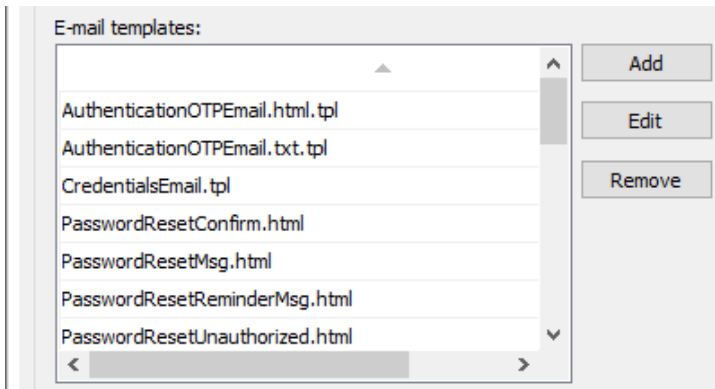
6. Enter an email address to send a test email to, then click **Send**. A confirmation message appears.
7. Click **OK** to dismiss the message. The **Send Test Email** button sends the email directly (synchronously). If you receive the test email, the SMTP configuration is correct.
8. In the **Address 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.



The "Address Book" interface shows a table with two columns: "Name" and "Address". There are several empty rows for adding new entries. To the right of the table is an "Add" button. Below the table is a "Remove" button. At the bottom of the interface, it says "Addresses available in E-mail Notification Event Rule Action".

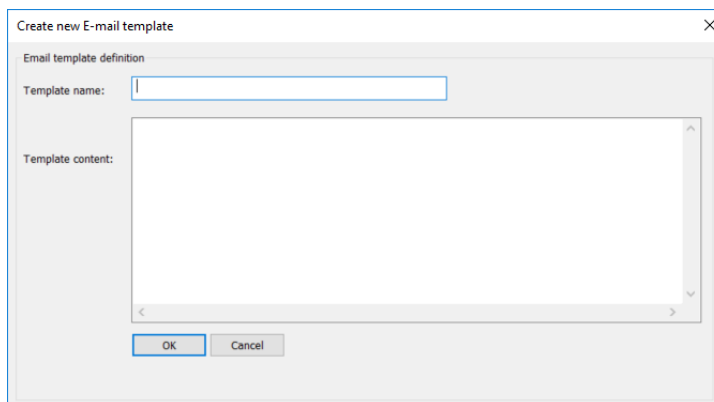
- To edit a name or address, click once to select the box, and then click again to activate the box.

- 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

- Click **Add**. The **Create New Email Template** dialog box appears.



- 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.
- Click **OK**.

To edit a template

- 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.
- The **Template name** cannot be edited.
- 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.")

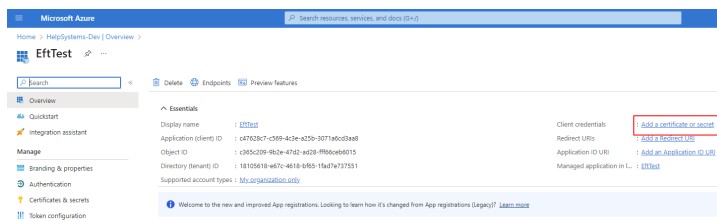
- Click **Apply** to save the settings on EFT.

Create a New Secret for OAuth

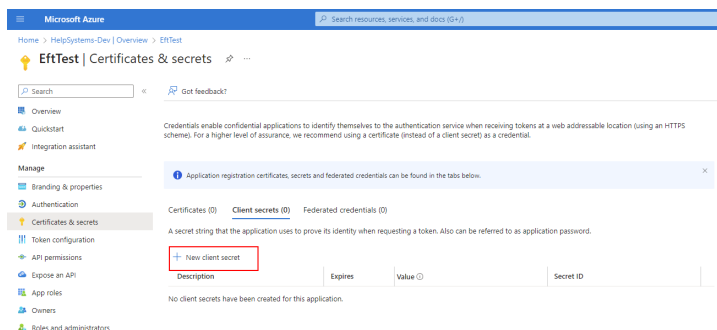
When OAuth (GOOGLE, OUTLOOK) is selected for authentication and emails are not being received, you may need to create a new secret for OAuth.

To create a new secret for OAuth

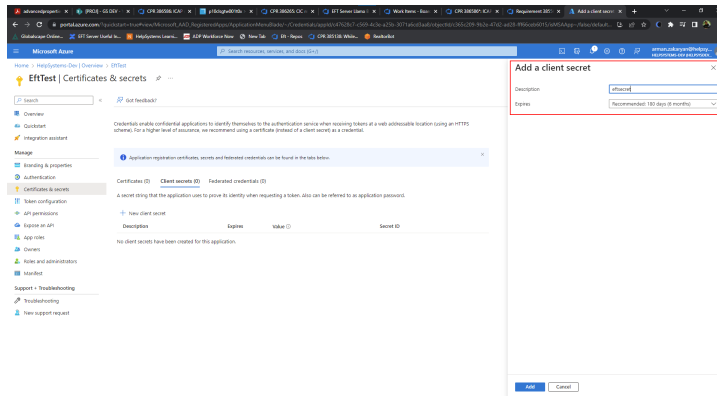
- Log into the Azure account
- In the **Overview** tab, then click **Add a certificate or secret**.



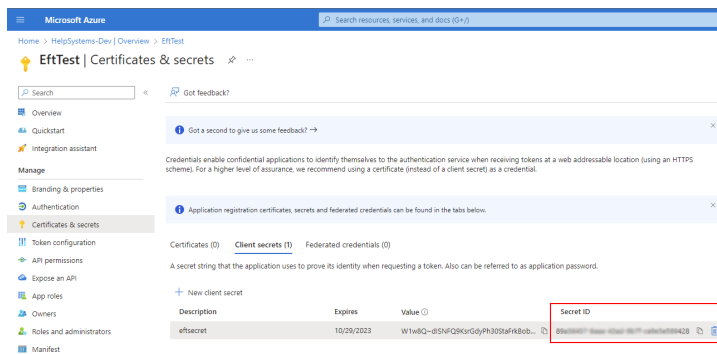
- Click **New client secret**.



- Give the secret a name



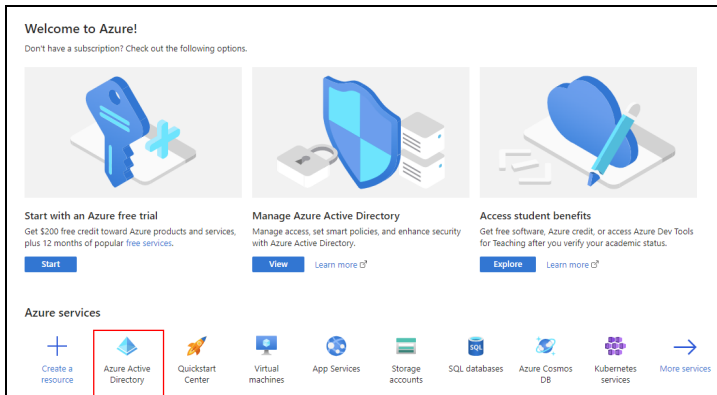
5. Save the secret value, as it will not be accessible later.



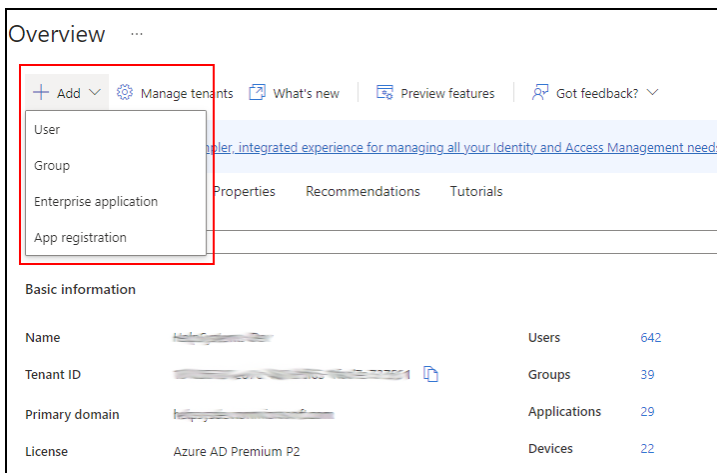
Create Admin Account for OAuth - Microsoft 365

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.

Register an application ...

* Name
The user-facing display name for this application (this can be changed later).
EftTest

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Help) Systems-Dev only - Single tenant

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform:

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- Provide a unique, user-facing name for the application, such as EFT. (You can change it later.)
- Under **Supported account types**, keep the default of **this organizational directory only**. Then click **Register**.
- On the application page (in this case, EftTest), next to Client credentials, click **Add a certificate or secret**.

EftTest ...

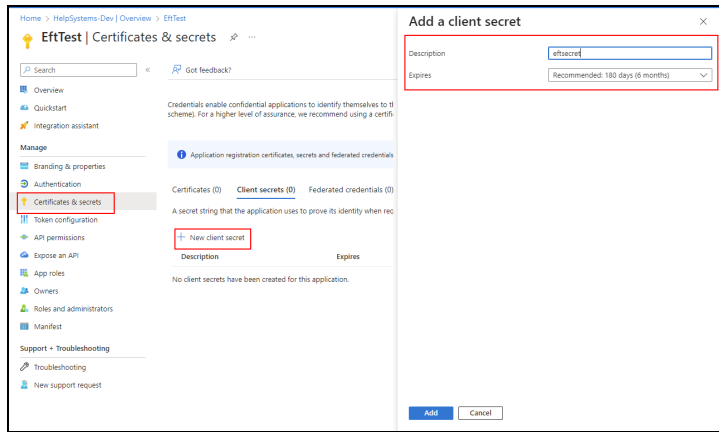
Search:

Overview | Quickstart | Integration assistant | Manage | Branding & properties | Authentication

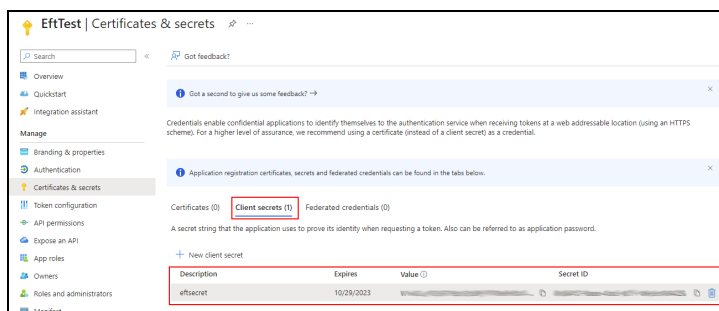
Essentials

Display name	: EftTest	Client credentials	: Add a certificate or secret
Application (client) ID	: c47628c7-c569-4c3e-a25b-3071a6cd3aa8	Redirect URIs	: Add a Redirect URI
Object ID	: c385c209-9b2e-47d2-ad28-fff66ceb6015	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 18105618-e67c-4618-bf65-1fad7e737551	Managed application in L...	: EftTest
Supported account types	: My organization only		

- The **Certificates & secrets** page appears. Click **New client secret**. The **Add a client secret** section appears.
- In the **Description** box, type a name for this secret.

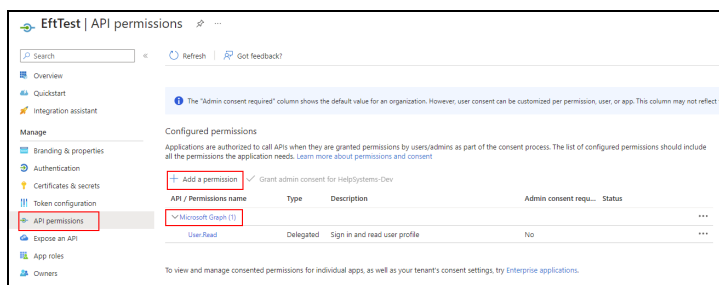


10. The secret appears under the **Description** on the **Client secrets** tab.



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.

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

mail

Permission	Admin consent required
MailboxSettings	
Mail (1)	
Mail.Read	Yes
Read mail in all mailboxes	
Mail.ReadBasic	Yes
Read basic mail in all mailboxes	
Mail.ReadBasic.All	Yes
Read basic mail in all mailboxes	
Mail.ReadWrite	Yes
Read and write mail in all mailboxes	
Mail.Send	Yes
Send mail as any user	

Add permissions Discard

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.

EFTDemo

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Essentials

Display name : EFTDemo

Application (client) ID : 9daf556a-ad3c-4538-99c4-3c758e37c7f6

Object ID : 1f87a77e-5a77-4e64-ab32-822b7f9f9e1b

Directory (tenant) ID : 020f3a33-fdb1-4dcd-b9af-e878aaf9d72

Supported account types : My organization only

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

LocalHost [127.0.0.1:1100] - Connected as admin [Started] - Globalscape - EFT

File Edit View Configuration Tools Reports Window Help

Report Status VFS Server

Default Server Group

MyOne

Specify your server settings for outbound e-mail notifications.

Email Server Settings

Authentication: Office 365 OAuth

Office 365 Account: jason@myone.com

Client ID: 9daf556a-ad3c-4538-99c4-3c758e37c7f6

Client Secret: *****

Tenant ID: 020f3a33-fdb1-4dcd-b9af-e878aaf9d72

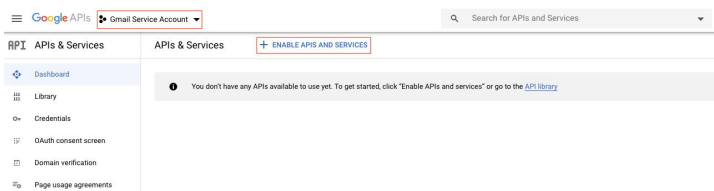
Create a Gmail/ Google Cloud Service Account

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/>.

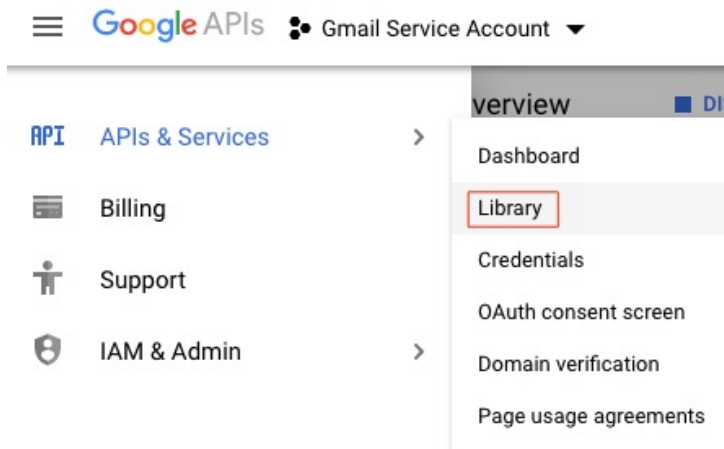
To create a Gmail service account

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**.

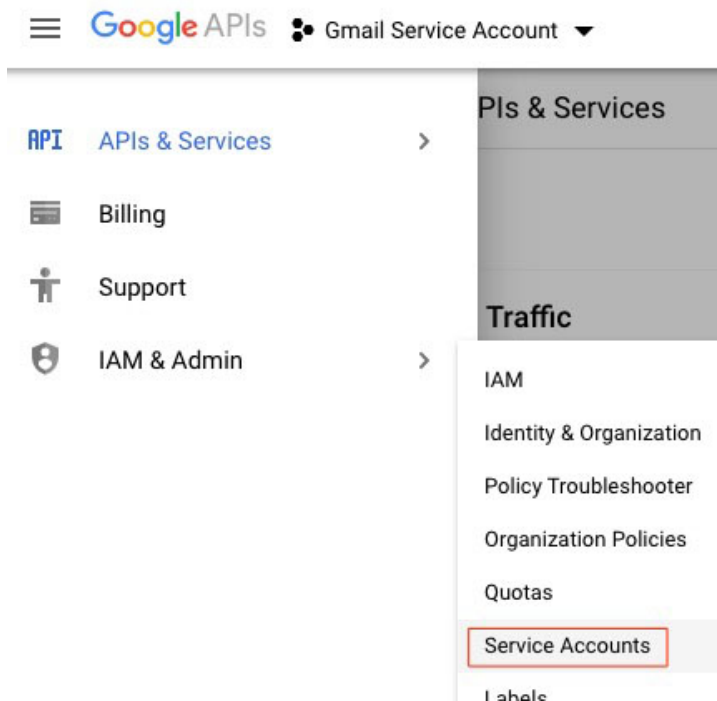


4. Click **+ ENABLEAPISANDSERVICES**.
5. In the API library, search for the following API sets. Click each set and then click Enable.
 - a. Gmail API
 - b. Google Calendar API
 - c. Contacts API
 - d. People API

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**.

← Create service account

1 Service account details

Service account name
Display name for this service account

Service account ID * ✕ ↺

Email address: <id>@gmail-service-account-363019.iam.gserviceaccount.com 📧

Service account description
Describe what this service account will do

CREATE AND CONTINUE

8. Fill in the details of the account and then click **CREATE AND CONTINUE**.

9. Click **Done**.

Service accounts ➕ CREATE SERVICE ACCOUNT 🗑 DELETE 🔑 MANAGE ACCESS 🔄 REFRESH

Service accounts for project "Gmail Service Account"

A service account represents a Google Cloud service or device, such as a VM running on Compute Engine VMs, App Engine apps, or software running outside Google. [Learn more about service accounts](#)

Organization policies can be used to restrict service accounts and block key service account features, such as automatic GHD Grants key creation updates, or the creation of service accounts entirely. [Learn more about service account organization policies](#)

Filter	Email	Status	Name	Description	Key ID	Key creation date	OAuth 2.0 Client ID	Actions
☐								- Manage details - Manage permissions Manage keys - View metrics - View logs - Disable - Delete
☐								
☐								

10. On the **Service accounts** page, under the **Actions** column, select the recently created service account then click **Manage keys**.

← Ebsta Service Account

DETAILS PERMISSIONS **KEYS** METRICS LOGS

Keys

⚠ Service account keys could pose a security risk if compromised. We recommend you [learn more](#).

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).

[Learn more about setting organization policies for service accounts](#)

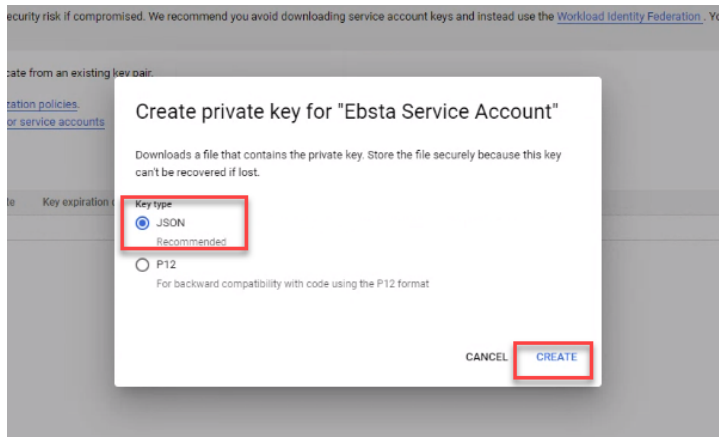
ADD KEY ▼

Create new key 👉

Upload existing key

Key creation date Key expiration date

11. On the account page, click **Create new key**.



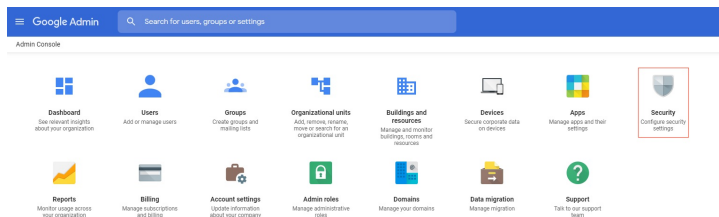
12. In the dialog box that appears, under **key type** click **JSON** then click **CREATE**.

NOTE: Capture the Client ID* as this will be needed later!

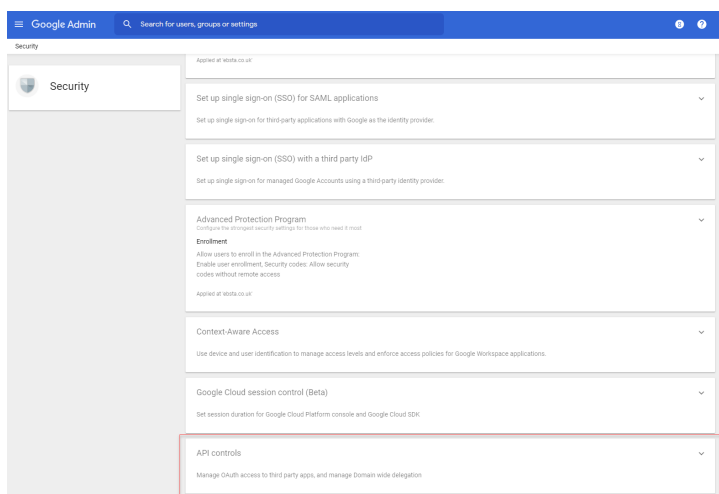
13. The JSON file should be downloaded to your computer. You must store this securely as it provides access to your resources. Click **Close**.

The next steps will enable the service account with Gmail.

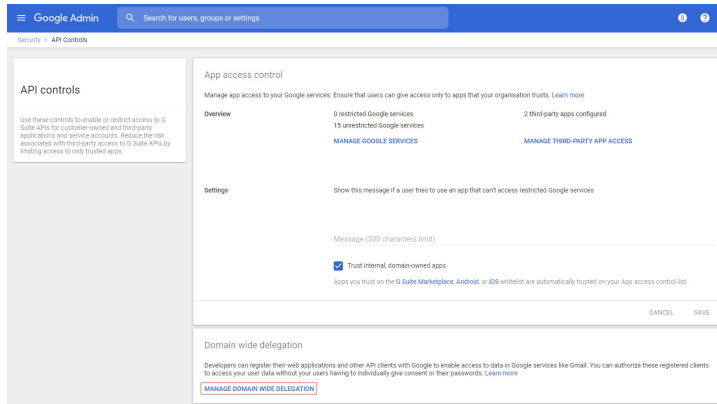
1. Login to the **Gsuite Admin Console**: <https://admin.google.com>, and then click the **Security** icon.



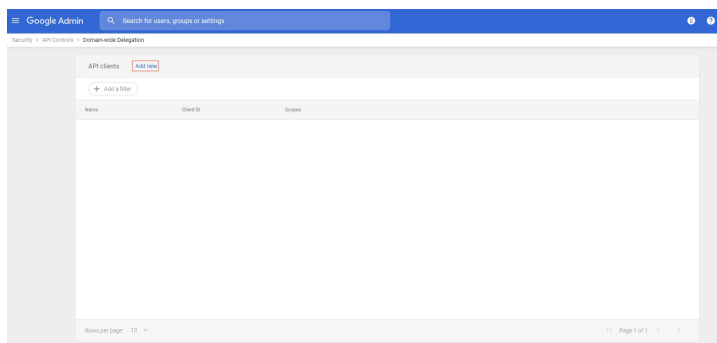
2. Under **Access and data control**, click **API controls**.



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.

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.

To request a trial extension

- Trial Extension Request

✕

Please complete the form below and then click Send. A request containing the following information will be emailed to Globalscape.

Name:

Company:

Email:

Phone:

Preview Request

After your request is processed, you will receive an email from Globalscape with further instructions.

Send

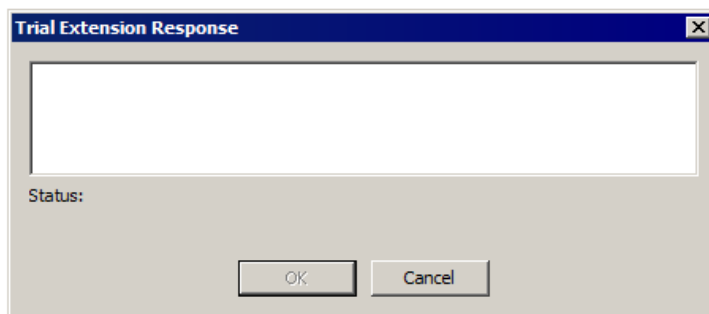
Cancel

- page: 132

- 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.

The screenshot shows a window titled 'Login Wizard' with a sub-header 'New Administrator Connection'. Below the header, the text 'Create a new connection to an EFT located on:' is displayed. There are two radio buttons: 'This computer' (selected) and 'A remote computer'. Below these, there are three input fields: 'Label' (containing 'Local-host'), 'Host address:', and 'Port:' (containing '1100'). At the bottom, there are two buttons: 'Next >' and 'Close'.

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.

The screenshot shows a window titled 'Login Wizard' with a sub-header 'EFT Administrator Login'. Below the header, the text 'Connect to EFT located on:' is displayed. There are two radio buttons: 'This computer' (selected) and 'A remote computer:'. To the right of 'A remote computer:' is a dropdown menu and a 'New' button. Below this, the text 'EFT administrator credentials:' is displayed. There are three input fields: 'Authentication:' (containing 'EFT Authentication'), 'Username:', and 'Password:'. At the bottom, there are two buttons: 'Connect' and 'Close'.

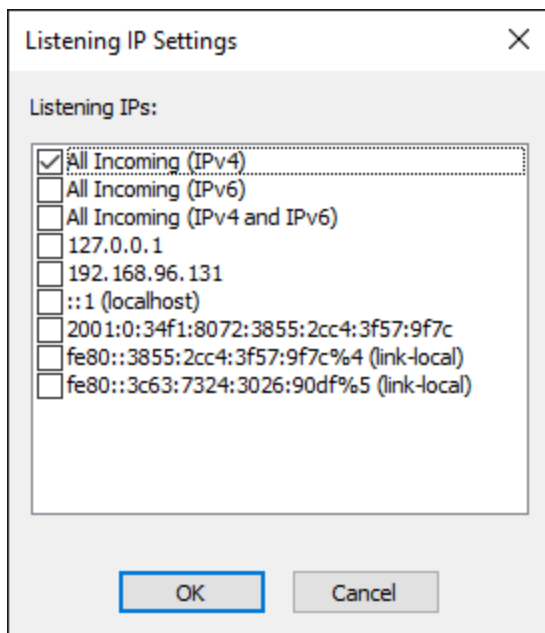
4. Click the **Authentication** box and specify the type of authentication to use for this login. Future connections will default to the authentication type that you specify during this initial login, but you can choose a different type. Authentication types include:
 - **EFT Authentication** - Choose 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.
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.

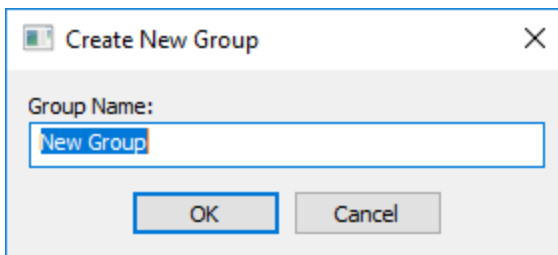
24. Click an option, then click **Finish**. If you chose FIPS mode for SSL and/or SSH, prompts appear explaining that EFT has entered FIPS mode. Click **OK** to dismiss the prompts.
25. If you chose **Run the Site Setup wizard now**, the Site Setup wizard **Welcome** page appears.
26. Refer to [Defining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

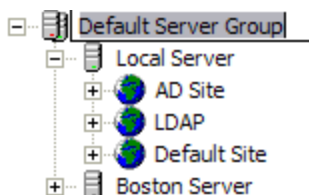
1. In the administration interface, [connect to EFT](#) and click the **Server** tab.
2. Click **File >New Server Group**. The **Create New Group** dialog box appears.



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.

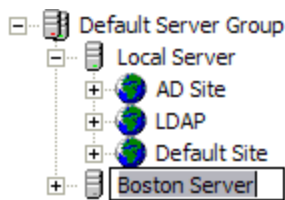
1. In the administration interface, [connect to EFT](#) and click the **Server** tab.
2. Click the Server Group that you want to delete.
3. Do one of the following:
 - On the main menu, click **File >Remove Server Group**.
 - Right-click the Server Group, and then click **Remove Server Group**.

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.

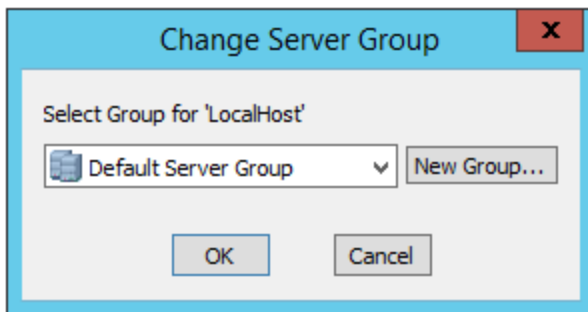
To delete a Server

When you delete a Server, you also delete all of its login information. You cannot undo this action.

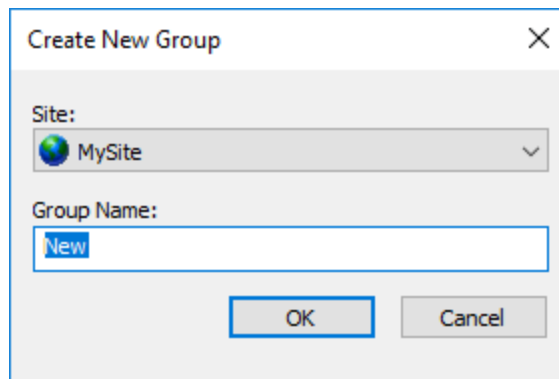
1. In the administration interface, [connect to EFT](#) and click the **Server** tab.
2. Do one of the following:
 - Right-click the Server node you want to delete, then click **Remove Server**.
 - Click the Server you want to delete, then on the main menu, click **File >Remove Server**.
3. A warning 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.



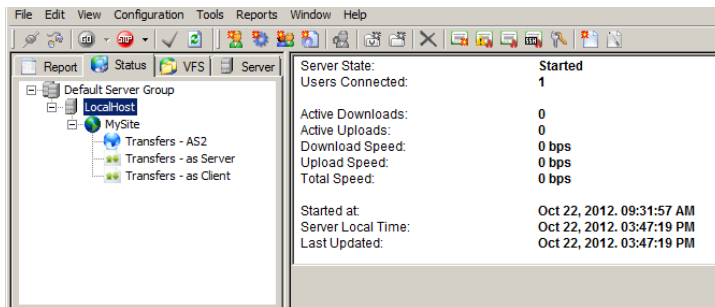
- b. Type a name for the new group, and then click **OK**. The **Change Server Group** dialog box reappears.
4. Click **OK**.

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.

EFT Messages and Templates

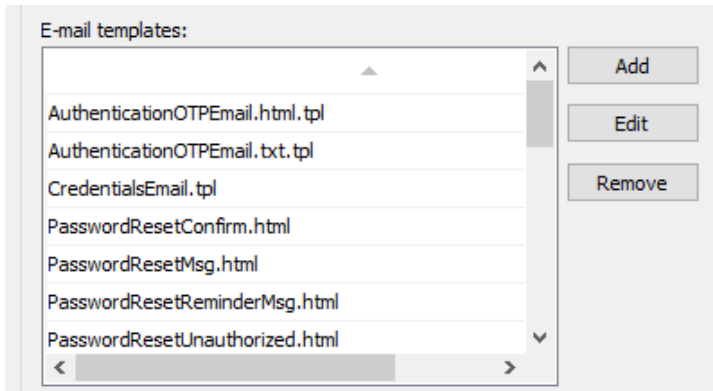
EFT generates several different types of messages during operation, such as event rule actions and server-level notifications. Some messages can be edited within the administration interface, others must be edited within a text file that you create, and others are hard coded and not editable. The various 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.

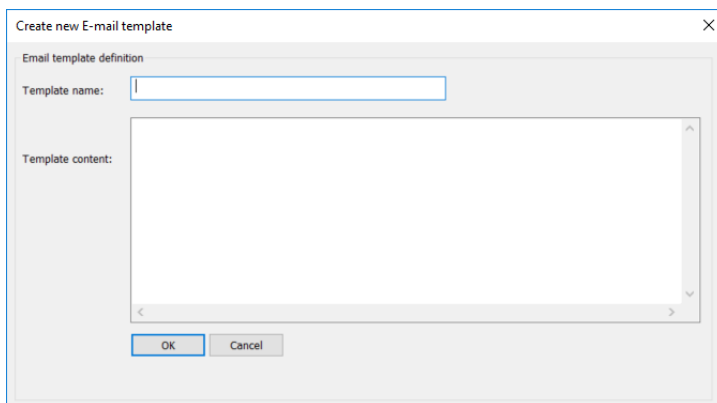
- EFT standalone template files were moved from the root of the local config directory to the "Templates" folder of the same location.
- EFT HA template were files moved from the root of each node's local config directory to the "Templates" folder in the shared config directory. All nodes' now share 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. Therefore any customization to these templates will be lost on upgrade but are backed-up.

Email Templates on the Server > SMTP Tab

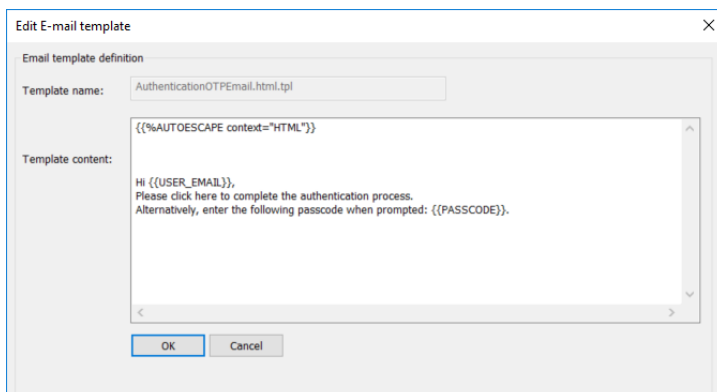
At the bottom of the **SMTP** tab is a table listing the email templates that you can edit or remove as well as add new templates.



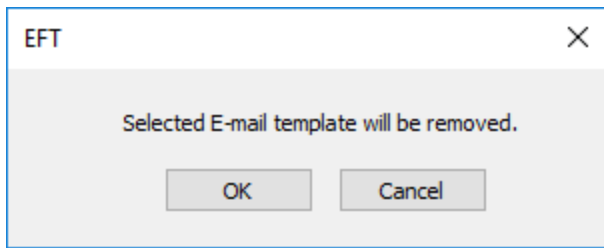
Add - Click **Add** to add a template. You can use HTML or plain text, and context variables and environment variables (with curly `{{ }}` brackets). View the existing templates for examples.



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.
- [WorkspacesOAEmail.html](#), [WorkspacesOAEmail.txt](#), [WorkspacesOAEmailWithSecureMB.html](#), [WorkspacesOAEmailWithSecureMB.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

Message	Description	
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 <i>n</i> 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.
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.)

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:

TLS Settings

SSL Compatibility

Minimum Protocol Version: ☒ TLSv1.3

Allowed ciphers:

☒ Select algorithms and order by preference

☒ Encryption [9/17]
☒ Message Authentication Code (MAC) [3/5]
☒ Key Exchange [3/4]
☒ Authentication [3/5]
☒ Cipher Suite Version [2/4]

☐ Manually specify algorithms in order of preference (advanced)

TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256

Example: ALL:!LOW:!EXPORT:!MD5:@STRENGTH (see documentation)

Resulting cipher list (25 of 25 selected):

Name	Version	Encryption	Mac	Key Exchange	Auth
☒ TLS_AES_256_GCM_SHA384	TLSv1.3	AESGCM(256)	AEAD	any	any
☒ ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	AESGCM(256)	AEAD	ECDH	ECDSA
☒ ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	AESGCM(256)	AEAD	ECDH	RSA
☒ AES256-GCM-SHA384	TLSv1.2	AESGCM(256)	AEAD	RSA	RSA
☒ TLS_CHACHA20_POLY1305_SHA256	TLSv1.3	CHACHA20/POLY1305(256)	AEAD	any	any
☒ ECDHE-ECDSA-CHACHA20-POLY1305	TLSv1.2	CHACHA20/POLY1305(256)	AEAD	ECDH	ECDSA
☒ ECDHE-RSA-CHACHA20-POLY1305	TLSv1.2	CHACHA20/POLY1305(256)	AEAD	ECDH	RSA
☒ TLS_AES_128_GCM_SHA256	TLSv1.3	AESGCM(128)	AEAD	any	any
☒ ECDHE-ECDSA-AES128-GCM-SHA256	TLSv1.2	AESGCM(128)	AEAD	ECDH	ECDSA
☒ ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	AESGCM(128)	AEAD	ECDH	RSA
☒ AES128-GCM-SHA256	TLSv1.2	AESGCM(128)	AEAD	RSA	RSA
☒ ECDHE-ECDSA-AES256-CCM8	TLSv1.2	AESCCM8(256)	AEAD	ECDH	ECDSA
☒ AES256-CCM8	TLSv1.2	AESCCM8(256)	AEAD	RSA	RSA
☒ ECDHE-ECDSA-AES256-CCM	TLSv1.2	AESCCM(256)	AEAD	ECDH	ECDSA
☒ AES256-CCM	TLSv1.2	AESCCM(256)	AEAD	RSA	RSA
☒ ECDHE-ECDSA-AES128-CCM8	TLSv1.2	AESCCM8(128)	AEAD	ECDH	ECDSA
☒ AES128-CCM8	TLSv1.2	AESCCM8(128)	AEAD	RSA	RSA
☒ ECDHE-ECDSA-AES128-CCM	TLSv1.2	AESCCM(128)	AEAD	ECDH	ECDSA
☒ AES128-CCM	TLSv1.2	AESCCM(128)	AEAD	RSA	RSA
☒ ECDHE-ECDSA-AES256-SHA384	TLSv1.2	AES(256)	SHA384	ECDH	ECDSA
☒ ECDHE-RSA-AES256-SHA384	TLSv1.2	AES(256)	SHA384	ECDH	RSA
☒ AES256-SHA256	TLSv1.2	AES(256)	SHA256	RSA	RSA
☒ ECDHE-ECDSA-AES128-SHA256	TLSv1.2	AES(128)	SHA256	ECDH	ECDSA
☒ ECDHE-RSA-AES128-SHA256	TLSv1.2	AES(128)	SHA256	ECDH	RSA
☒ AES128-SHA256	TLSv1.2	AES(128)	SHA256	RSA	RSA

FIPS mode was unchanged:

TLS Settings

SSL Compatibility

Minimum Protocol Version: ☒ TLSv1.2

Allowed ciphers:

☒ Select algorithms and order by preference

☒ Encryption [4/5]
☒ Message Authentication Code (MAC) [3/4]
☒ Key Exchange [2/7]
☒ Authentication [2/5]
☒ Cipher Suite Version [1/2]

☐ Manually specify algorithms in order of preference (advanced)

TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256

Example: ALL:!LOW:!EXPORT:!MD5:@STRENGTH (see documentation)

Resulting cipher list (12 of 12 selected):

Name	Version	Encryption	Mac	Key Exchange	Auth
☒ ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	AESGCM(256)	AEAD	ECDH	ECDSA
☒ ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	AESGCM(256)	AEAD	ECDH	RSA
☒ AES256-GCM-SHA384	TLSv1.2	AESGCM(256)	AEAD	RSA	RSA
☒ ECDHE-ECDSA-AES128-GCM-SHA256	TLSv1.2	AESGCM(128)	AEAD	ECDH	ECDSA
☒ ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	AESGCM(128)	AEAD	ECDH	RSA
☒ AES128-GCM-SHA256	TLSv1.2	AESGCM(128)	AEAD	RSA	RSA
☒ ECDHE-ECDSA-AES256-SHA384	TLSv1.2	AES(256)	SHA384	ECDH	ECDSA
☒ ECDHE-RSA-AES256-SHA384	TLSv1.2	AES(256)	SHA384	ECDH	RSA
☒ AES256-SHA256	TLSv1.2	AES(256)	SHA256	RSA	RSA
☒ ECDHE-ECDSA-AES128-SHA256	TLSv1.2	AES(128)	SHA256	ECDH	ECDSA
☒ ECDHE-RSA-AES128-SHA256	TLSv1.2	AES(128)	SHA256	ECDH	RSA
☒ AES128-SHA256	TLSv1.2	AES(128)	SHA256	RSA	RSA

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 module](#) supports 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-ftptext2-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 reference](#) for 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, <i>imauser@me.com</i>)	ASCII only (7-bit)	ASCII	ASCII	Unicode
EFT	Email usernames (for example, <i>Ima User</i>)	Unicode	Unicode	Unicode	Unicode

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).

Configuring SSL

The topics below provide information regarding configuring SSL.

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.

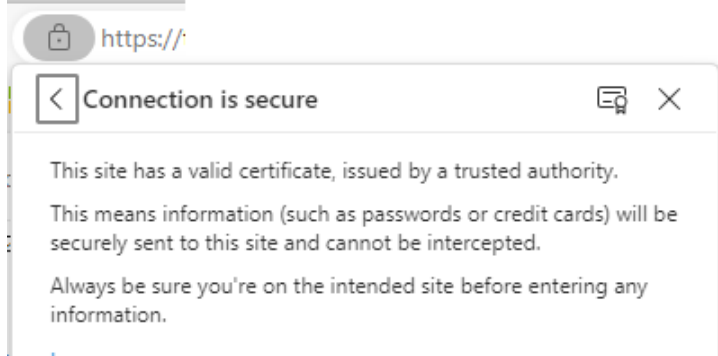
EFT's SSL implementation uses all the SSL configuration made on the **Server > Security** tab for all SSL operations, including Event Rules.

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.

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.

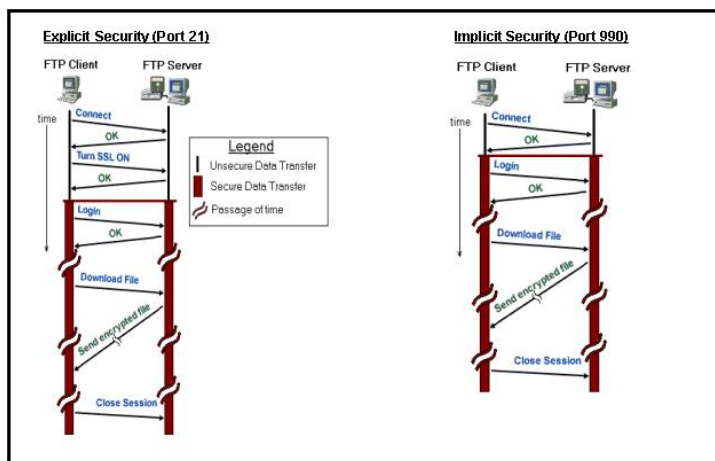
Explicit Security: To establish the SSL link, explicit security requires that the FTP client issue a specific command to the FTP server after establishing a connection. The default FTP server port is used. This formal method is documented in [RFC 2228](#).

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.

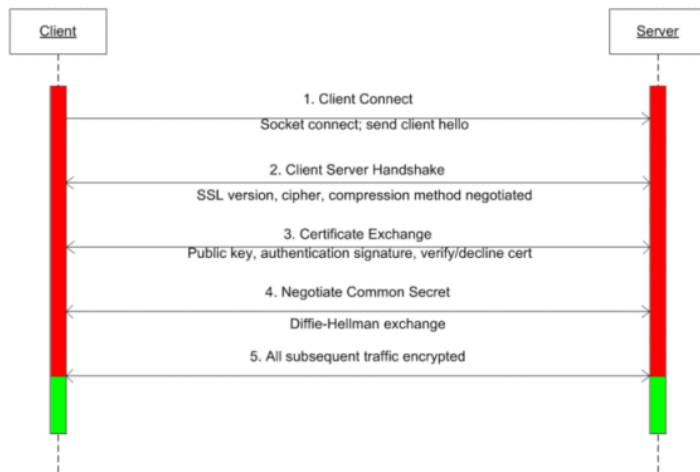
Because implicit SSL has a dedicated port strictly used for secure connections, implicit SSL connections require less overhead when you establish the session. There are various FTP servers that support this mode, including EFT, RaidenFTPD, IBackup's FTP server, and others.

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.

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)

Encoding				
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

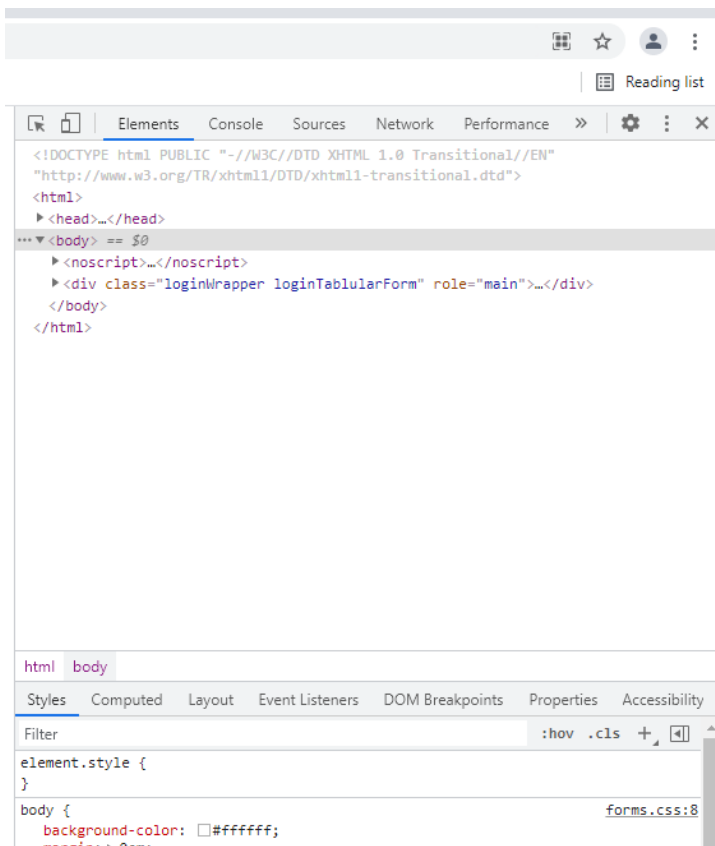
EFT v8.0.6 and later support the TLS 1.3 protocol with OpenSSL v1.1.1.

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.)

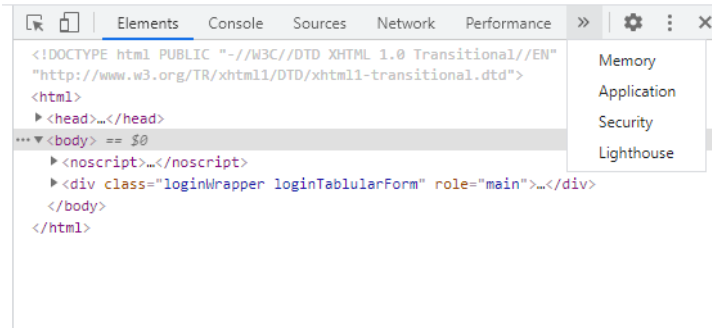
You can use developer tools in the browser to verify that the Web Transfer Client is using TLS.

To verify that TLS 1.3 is being used

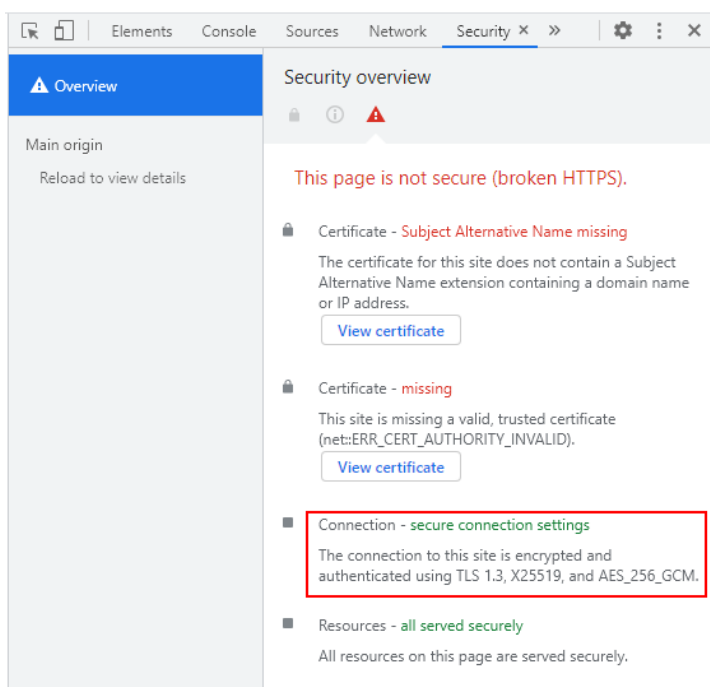
1. Open your browser and navigate to the Web Transfer Client URL, such as <https://localhost/Web/Account/Login.htm>.
2. Do not log in.
3. Maximize the browser window.
4. Press F12 on your keyboard.



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.

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.

The screenshot shows a dialog box titled "Certificate Notification Expiration". It has a close button (X) in the top right corner. Inside the dialog, there are four checkboxes:

- ☐ Send an email upon expiration
- ☐ Send an email 30 days prior to expiration (the number 30 is in a spinner box)
- Recipients list:
- ☐ Send copy to user associated with this event (if applicable)

 At the bottom, there are two buttons: "OK" and "Cancel".

- 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 server](#) needs to be configured properly.

6. Click **OK** to close the dialog box.
7. 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.

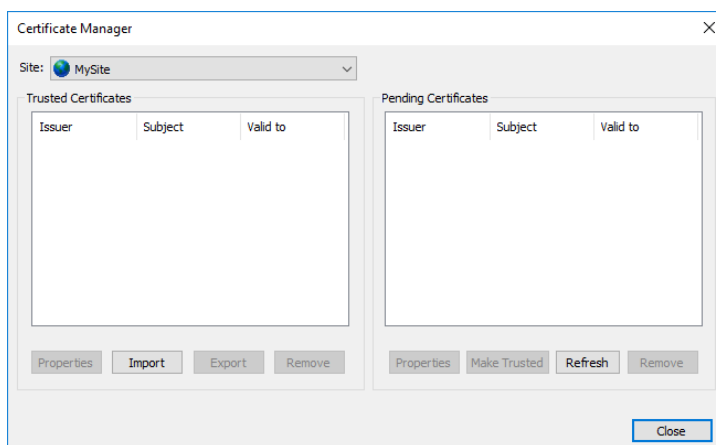
The way you access the intermediate and root certificates, as well as the format of those certificates, might differ between signing authorities.

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.

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
 - 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.

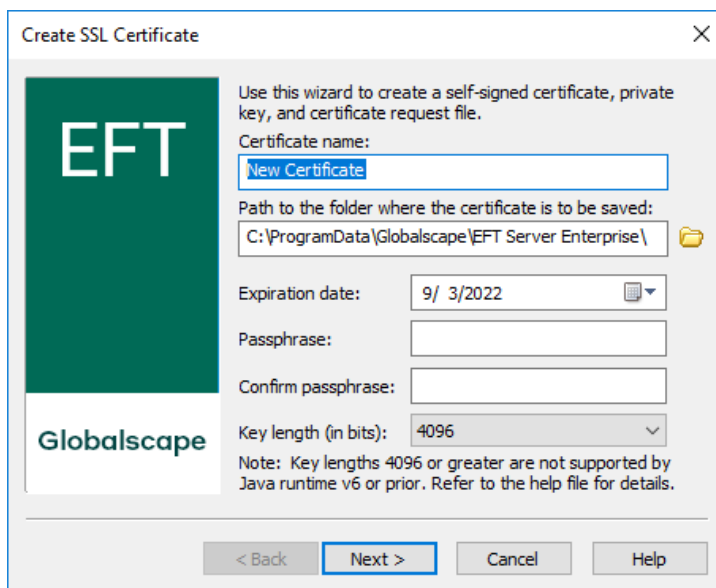
The current build of EFT does not provide a mechanism to "decrypt" the file created with the signing process.

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.



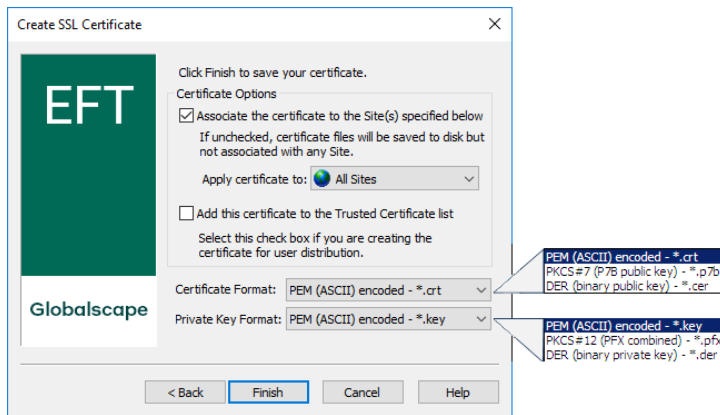
2. In the **Certificate name** box, specify the name (up to 256 characters) of the certificate that will be generated.
3. In the **Path** box, specify the path to the folder in which the certificate is to be saved. The wizard saves each of the files in this folder.

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.

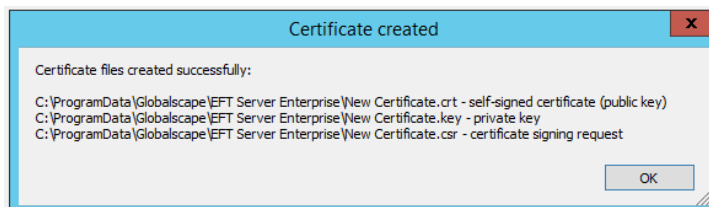
8. In the **City/Town** box, provide the name of your city, town, or other locality.
9. In the **State/Province** box, provide the name of the state or province.
10. In **Organization** box, provide the name of your organization, or any other designator.
11. In the **Common Name** box, provide the common 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.
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 180](#) and [Enabling SSL on the Server on page 179](#) for instructions for using the SSL certificate.

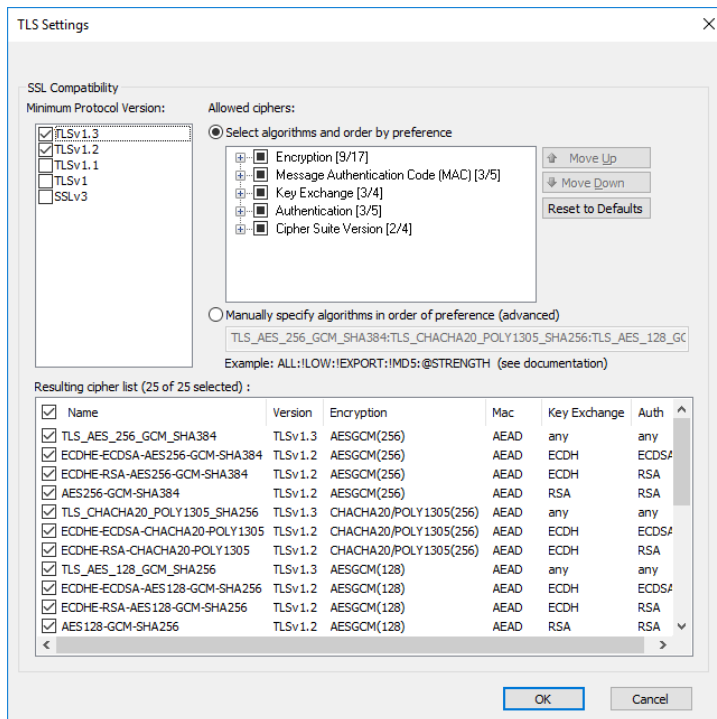
Enabling SSL on the Server

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](#).

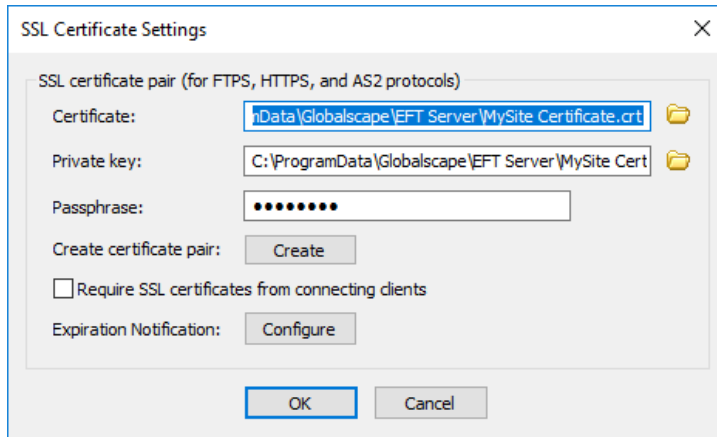
If you require certificates from connecting clients before they can connect, then their certificate must be in the Trusted Certificates Database or signed by a certificate in the Trusted Certificate Database.

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.

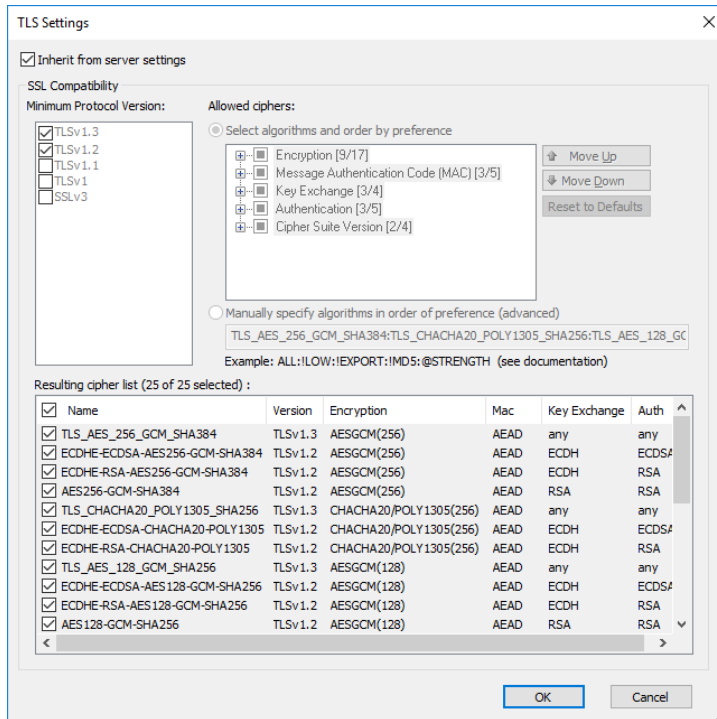
5. Click **OK** to close the dialog box.
6. Click **Apply** to save the changes to EFT.

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 167](#) and [Enabling SSL on the Server on page 179](#) for more information on specifying these settings.

Configuring SSL Authentication for a Settings Template or User Account

SSL must first be enabled on the [Site](#) and [Server](#). SSL authentication can then be enabled for a Settings Template and/or for each user.

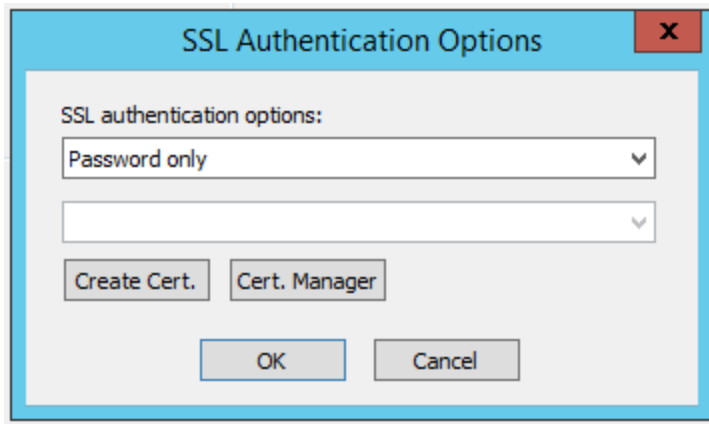
If you require certificates from connecting clients before they can connect, then their certificate must be in the Trusted Certificates Database or signed by a certificate in the Trusted Certificate Database.

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:

```

1 Bag Attributes
2   localKeyID: 01 00 00 00
3   friendlyName: 633438695139008599
4   Microsoft CSP Name: Microsoft Base Cryptographic Provider v1.0
5 Key Attributes
6   X509v3 Key Usage: 10
7 -----BEGIN RSA PRIVATE KEY-----
8 MIICXQIBAAKBgQC2izwuMKf1SVlks3KNcEN5oagzvGnwjLL9HOpBaqd9gkcHzZmc
9 TlG1LreKwaOxbr2BMIEHkYC2GzVjBcQUSz/QOYY0Brbg+hoBvrCt547cPSqSBQdL
10 BLebYWEqua7R25R80yiMfTwZwQB0+DHD+pD1XAB9AN/ENjGyc4VPU+A6/QIDAQAB
11 AoGBAKGJZzEM16T1Stk1P2rQfLWHC7z0r98x8zax2Nk404zqm4bZN2Uuf/QAWWVx
12 27yn7aMkVBppdTgxrbW6JYE78fQH2kx5D3RtJYpgULmYkp2MHG1gfuPVtMVRs+R
13 JuXP47ysQVR0GMwUftgANpov9Mx/1GU36CF/oiG7cjIyMpELAkEA4sDJqFvKofGF
14 M0sUCU0L2A+RRjKNQ3bTgt5o8LNU6uRh3ztbsKB+J+FvNArRWU4Ftgn3U7q7BwT9
15 Aabte2pnRwJBAM4WsaKsnvTEM/oByMbFJ0360AbLSx7e3q44z19xAt1WwPh/mn7
16 Rd6oKdHf61ML+kfGGFzHV99UCrca9aFeNZsCQDQg8m5bhcv11bMTJ3J2CjtW0YNe
17 B1JapiwIPQoQf4GmPrBtW56HZ4AfoiXG1CDBH0TN5a81si50NWU1W0tpLtkLAKBq
18 jVkyXkWNd4BAFoQUIQL9U1wT5y/juh8vvLcWqXtrm2wo74WZkC7spkyFOTIRlf0F
19 AGrALWdFWtJfcVTmJatZAKBgG3Uk6sT0jdWONbkG57DRITMnrHjJ2xuL00dEfjS
20 e3EumP0iaY7m6c/2EqrB+wRD1/2HUaBId0u2woDis30T
21 -----END RSA PRIVATE KEY-----
22 Bag Attributes
23   localKeyID: 01 00 00 00
24   subject=/CN=EDI Connector Cert
25   issuer=/CN=EDI Connector Cert
26 -----BEGIN CERTIFICATE-----
27 MIIBrjCCARegAwIBAgIBATANBgkqhkiG9w0BAQUFADAdMRswGQYDVQQDExJFREkg
28 Q29ubmVjdG9yIEN1cnQwHncNMDgwNDE1MjAxODM0MWhcNMDkwNDEOMjAxODM0MjAd
29 MRswGQYDVQQDExJFREkgQ29ubmVjdG9yIEN1cnQwZ8wDQYJKoZIhvcNAQEBBQAD
30 gYOAAMIGJAoGBALaLPC4wp/VJWWSzcolwQ3mhqD08afCMsv0fSkFqp32CRwfNmZxP
31 UaIut4pZ07FtHYEwgQeRgLYbNWMFxBRLP9A5hg4GtuD6GgG+sK3njtw9KpIFB0sE
32 t5thYSq5rStHb1Hw7KIx9PBnBAE74McP6kPVCaHOA38Q2MbJzhU9T4Dr9AgMBAAEw
33 DQYJKoZIhvcNAQEBBQADgYEALdwDjY/epA6t63cAcLf2Vhv+hRSh+wgkxX6x4IPA
34 jL0Jyx0rTPKEcq1Md8NMxi0hGnuhR5hl4IpSvQ1W92Xeq5WMMfikiLfdh0BczgBjX
35 KplhndxyWFeJ6o/9xmSKR0ctNPi+/n/Y9ADNaP2iz+sgD0gicLaPaljGMDgxEUN
36 MLY=
37 -----END CERTIFICATE-----

```

- 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-----
```

- 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.

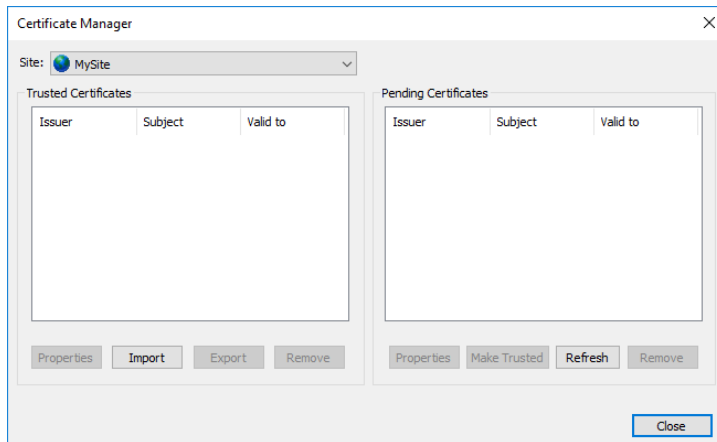
Importing a Certificate

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 Certificate**. 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.

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.

The screenshot shows a dialog box titled "Certificate Notification Expiration". It has a close button (X) in the top right corner. Inside the dialog, there are four checkboxes:

- ☐ Send an email upon expiration
- ☐ Send an email 30 days prior to expiration
- Recipients list: [text input field]
- ☐ Send copy to user associated with this event (if applicable)

 At the bottom of the dialog are two buttons: "OK" and "Cancel".

- 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 server](#) needs to be configured properly.

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

Signing a Certificate

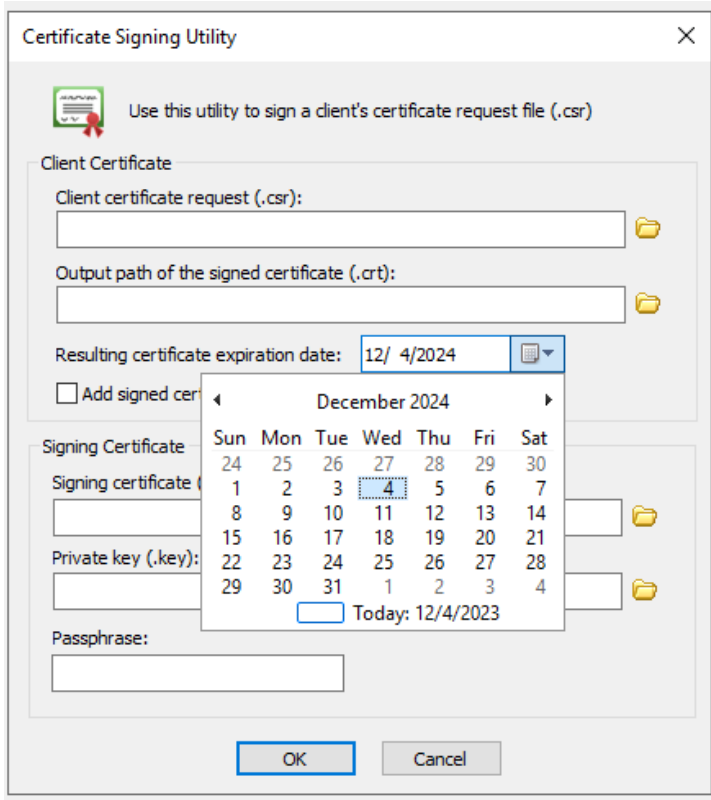
EFT can sign certificate requests created by other clients. Typically, the client certificate request is signed with the certificate created for EFT. If a certificate from the FTP server's Trusted Certificates database is used to sign client certificates, then all certificates you sign are automatically 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.



The **Certificate Signing Utility** dialog box is shown. It contains the following fields and controls:

- Client Certificate** section:
 - Client certificate request (.csr): [Text box with folder icon]
 - Output path of the signed certificate (.cert): [Text box with folder icon]
 - Resulting certificate expiration date: 12/ 4/2024 [Dropdown arrow]
 - ☐ Add signed cert
- Signing Certificate** section:
 - Signing certificate: [Text box with folder icon]
 - Private key (.key): [Text box with folder icon]
 - Passphrase: [Text box]

A calendar is open over the expiration date field, showing December 2024. The date 4 is selected. Below the calendar, it says "Today: 12/4/2023".

Buttons: **OK** and **Cancel**.

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-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](#).

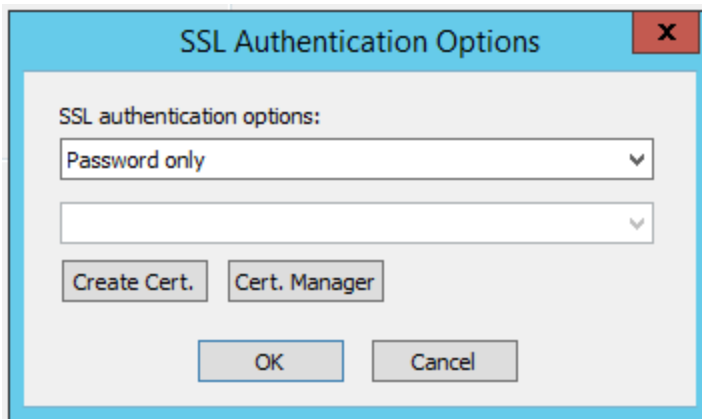
To specify SSL certificate-based logins for the Site

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.

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.

The screenshot shows the 'Connections' tab in the EFT administration interface. The 'Listener Settings' section is active, showing a list of protocols with their respective ports and checkboxes. The 'Listening IP addresses' is set to 'All Incoming (IPv4)'. The 'Domain' is set to 'localhost'. The 'AS2' checkbox is unchecked, and the 'Require additional factor for HTTP/S auth' is set to 'OTP - Email delivery'. The 'Allow Globalscape Mobile Transfer Client (MTC) over HTTPS' checkbox is checked. The 'Event Rule invoke over WS/SOAP (uses HTTPS port)*' checkbox is unchecked. The 'Redirect all plaintext HTTP traffic to HTTPS*' checkbox is unchecked. The 'Enable HSTS' checkbox is checked. The 'Enable Proxy Protocol for all protocols enabled on this Site' checkbox is unchecked. The 'SSL certificate settings' and 'SSL security settings' sections are visible, each with a 'Configure' button. The 'Network Usage and Security Settings' section is also visible, with 'Connection limits', 'IP access/ban list', and 'Denial of Service settings' each having a 'Configure' button.

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](#)

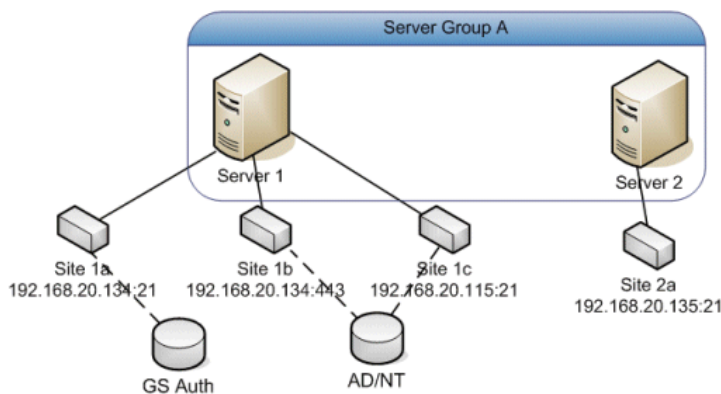
Site Configuration

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

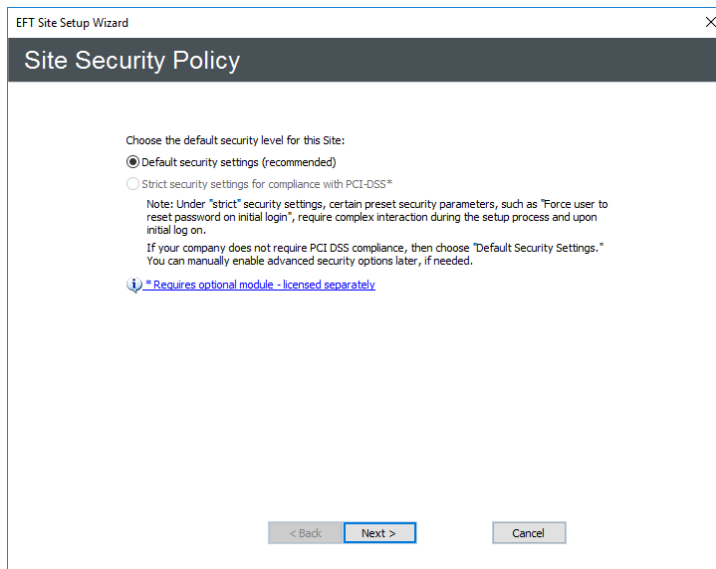
Creating a Site

A *Site* is how you connect to EFT. This topic describes how to create the connection, including IP address, port, and so on.

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.

EFT Site Setup Wizard

Site Label and Listening IP

Configure a Site for servicing inbound connections.

To begin, provide a name for this Site. Create a unique, distinguishing label, as it is possible to have more than one Site running on the same physical server.

Site label:

If you have more than one IP address and plan on running multiple Sites on this server, specify the IP address this Site should listen on. Alternatively, choose **All Incoming** to service all IP addresses assigned to this computer.

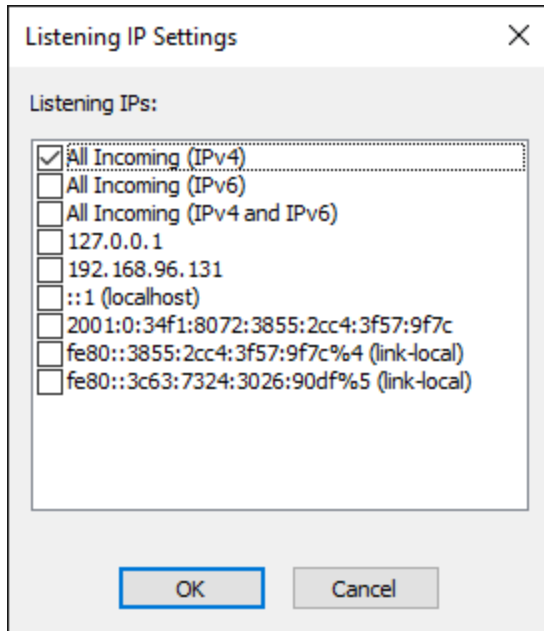
Listening IPs:

< Back Next > Cancel

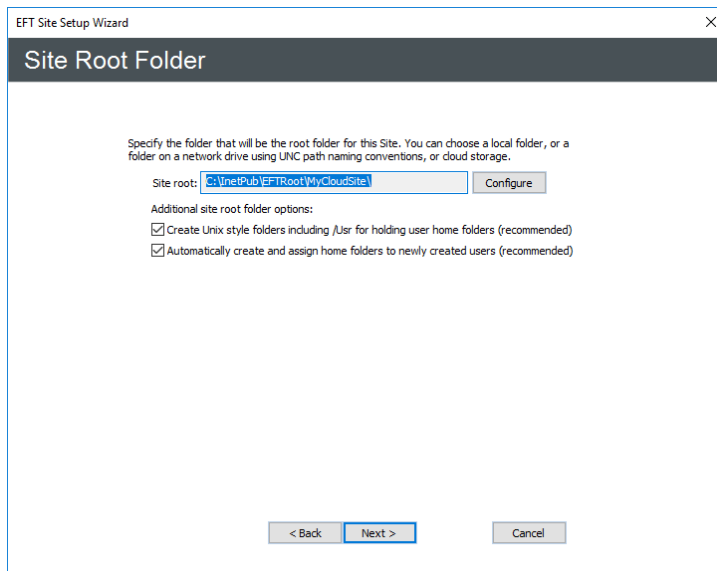
4. In the **Site label** box, type a distinguishing name for the Site. `MySite` appears by default, but you can change this to anything you want.

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.

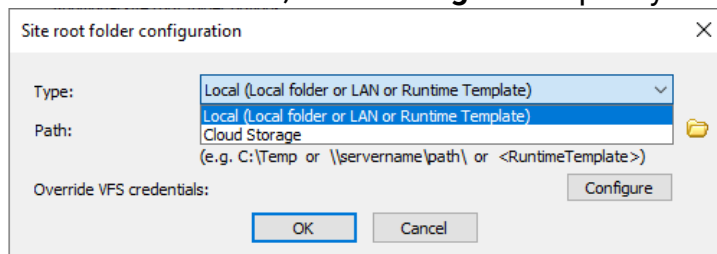
5. Next to the **Listening IPs** box, click **Configure**. The **Listening IP Settings** dialog box appears.



- 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.

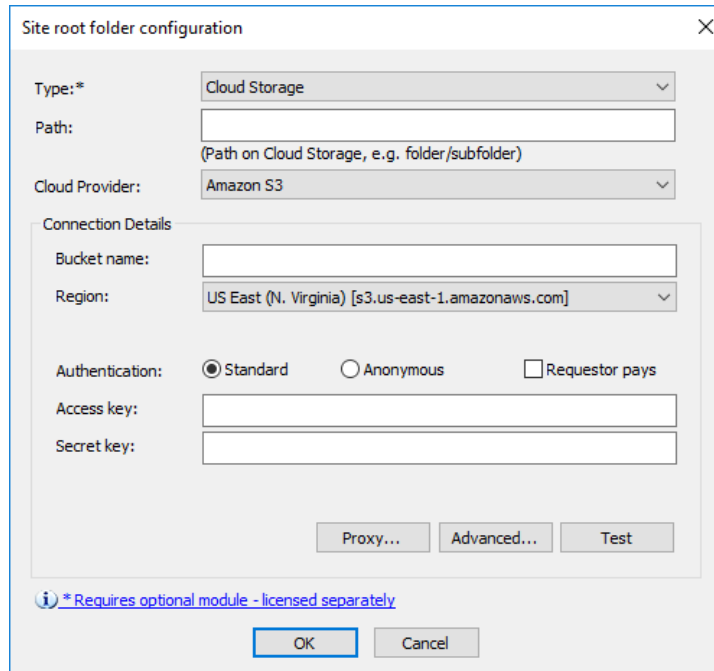


8. In the **Site root** box, click **Configure** to specify the root folder.



- 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.

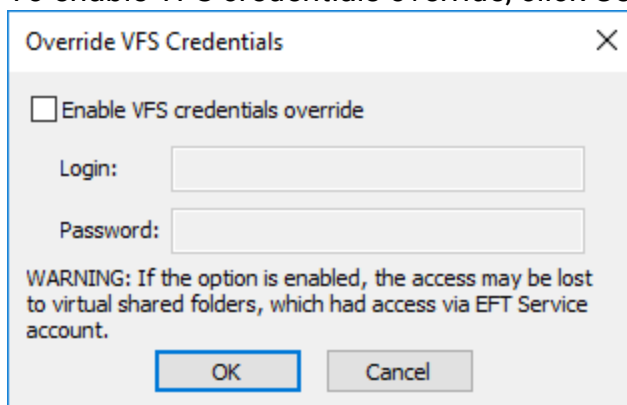
NOTE: The Cloud Connector Module (CCM) is required for all cloud-based activities.



The 'Site root folder configuration' dialog box contains the following fields and options:

- Type:** Cloud Storage (dropdown)
- Path:** (text input field)
- Cloud Provider:** Amazon S3 (dropdown)
- Connection Details:**
 - Bucket name:** (text input field)
 - Region:** US East (N. Virginia) [s3.us-east-1.amazonaws.com] (dropdown)
 - Authentication:** Standard (selected), Anonymous, Requestor pays (checkbox)
 - Access key:** (text input field)
 - Secret key:** (text input field)
- Buttons:** Proxy..., Advanced..., Test
- Footer:** * Requires optional module - licensed separately (with an information icon), OK, Cancel

- 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**.



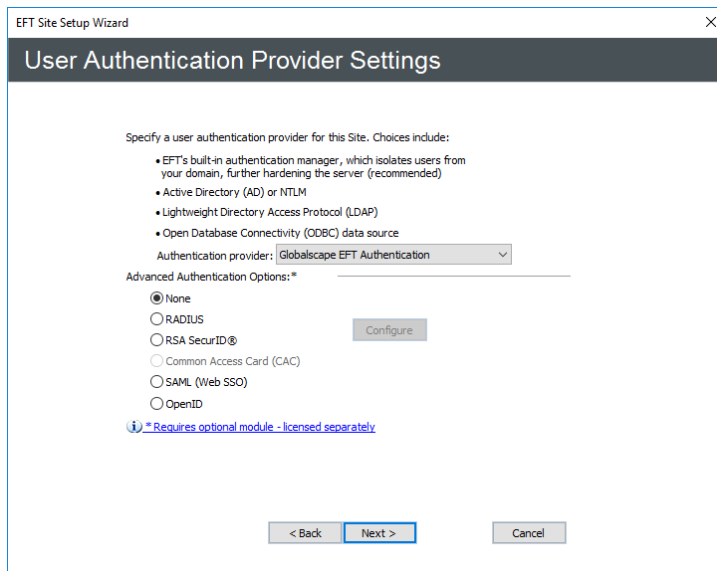
The 'Override VFS Credentials' dialog box contains the following fields and options:

- Enable VFS credentials override:** (checkbox, currently unchecked)
- Login:** (text input field)
- Password:** (text input field)
- WARNING:** If the option is enabled, the access may be lost to virtual shared folders, which had access via EFT Service account.
- Buttons:** OK, Cancel

- Select the **Enable** check box, then 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.)

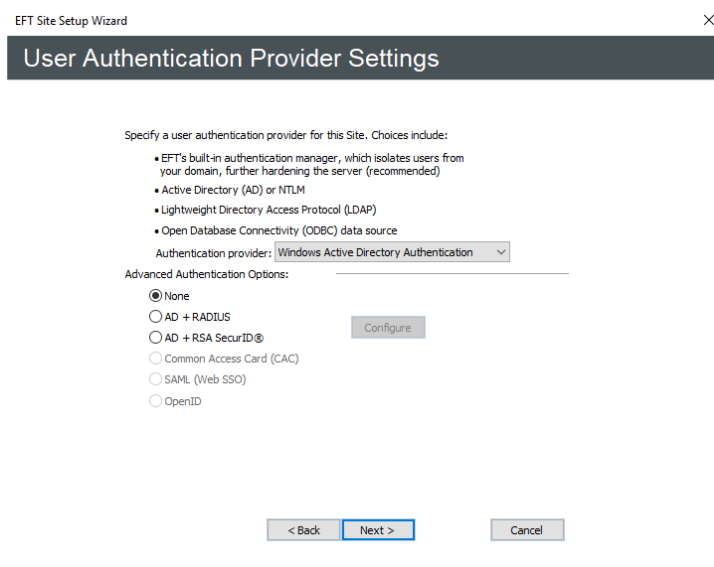
- [Globalscape EFT Authentication](#) - Does not rely on outside sources for user information. All information in the authentication database is protected from the operating system, contained within EFT, and can only be modified through the administration interface.
- [Windows Active Directory \(AD\) 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

- Verify that **Globalscape EFT Authentication** is specified, and then The **EFT Server Authentication** page appears.
- 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.
- Click **Next**. The [Perimeter Network Security](#) page appears.

For Windows Active Directory Authentication

- 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.
- 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.

The screenshot shows the 'Windows Authentication Options' window from the EFT Site Setup Wizard. It has a title bar 'EFT Site Setup Wizard' and a close button. The window is divided into sections for configuration.

Type: ☒ Active Directory ☐ Local System Accounts

Domain: ☒ Default ☐ Specify:

Group: ☒ Everyone ☐ Specify:

Separate multiple groups by using a comma. E.g., Accounting, Sales.

Advanced

Use this user attribute as account name:

User list refresh interval:

☐ Synchronize user(s) only after they first attempt to log in

☒ Access permissions are managed by Windows

When creating home folders for newly added users:

☐ Create a virtual folder pointing to the user's home folder as defined in his/her AD profile

☐ Keep user's home folder in sync with AD profile folder

☒ Create a physical folder under the site root folder using the user's login name

☐ Don't include domain attribute in folder name, e.g. /jsmith, rather than /domain.jsmith

- 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 [VFS](#) subtree 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 users](#) is 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

- If you are using Common Access Card (CAC) authentication, click **Common Access Card (CAC) authentication**. (The **Configure** button applies only to RADIUS and RSA.)
- In the **Authentication type** list, click **LDAP Authentication**, then click **Next**. The **LDAP Authentication** page appears.

The screenshot shows the 'LDAP Authentication' window of the 'EFT Site Setup Wizard'. The window has a title bar with a close button. The main area contains the following fields and controls:

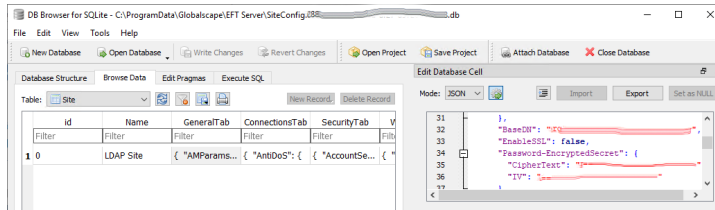
- Server:** A text input field.
- Port:** A text input field with the value '389'.
- Base DN:** A dropdown menu with a 'List DN's' button next to it.
- User filter:** A text input field with the value '(objectClass=person)'.
- Login attribute:** A text input field with the value 'cn'.
- Authentication mode:** Two radio buttons: 'Simple login' and 'Anonymous login' (which is selected).
- Username:** A text input field.
- Password:** A text input field.
- Bind using SSL:** A checkbox that is unchecked.
- Advanced:** A button.
- Test:** A button.
- User list refresh interval:** A dropdown menu with the value 'Use server specified interval'.
- Synchronize user(s) only after they first attempt to log in:** A checkbox that is unchecked.
- Navigation:** At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- In the **Server** box, type the **Server** name or IP address.
- In the **Port** box, keep the default port 389 or specify a different port used by your LDAP server.
- 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 DN's** to complete the box automatically or select from a list.
- In the **User Filter** box, type the search filter information. Refer to [Advanced LDAP Filtering](#) for a detailed explanation of LDAP filtering.
- 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`
- 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
```

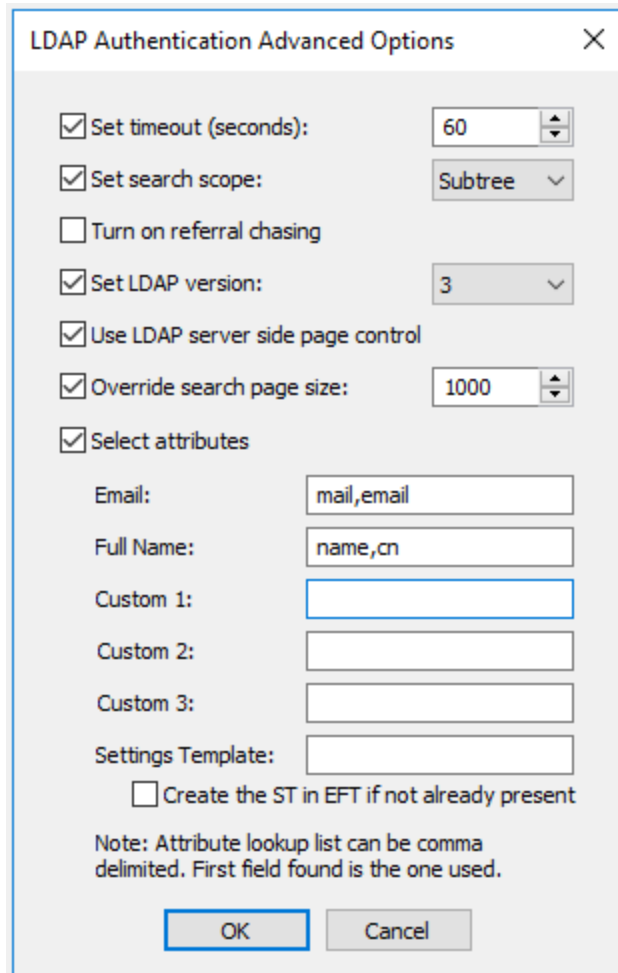
The LDAP bind password is encrypted and stored in the SQLite file,
..\ProgramData\Globalscape\EFT Server\SiteConfig.nnnnnnnnn.db



- 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.



The dialog box titled "LDAP Authentication Advanced Options" contains the following settings:

- ☒ Set timeout (seconds): 60
- ☒ Set search scope: Subtree
- ☐ Turn on referral chasing
- ☒ Set LDAP version: 3
- ☒ Use LDAP server side page control
- ☒ Override search page size: 1000
- ☒ Select attributes
 - Email: mail,email
 - Full Name: name,cn
 - Custom 1:
 - Custom 2:
 - Custom 3:
 - Settings Template:
 - ☐ Create the ST in EFT if not already present

Note: Attribute lookup list can be comma delimited. First field found is the one used.

Buttons: OK, Cancel

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 Details](#) for 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

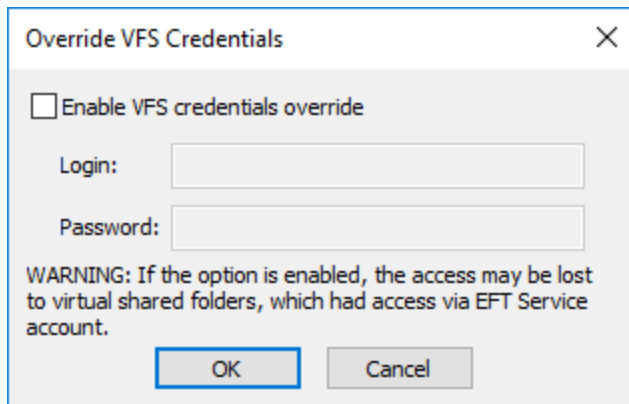
- a. Click **Next**. The **ODBC Authentication** page appears.

The screenshot shows the 'ODBC Authentication' window of the 'EFT Site Setup Wizard'. The window has a title bar with 'EFT Site Setup Wizard' and a close button. The main content area is titled 'ODBC Authentication'. Below the title, there is a text box labeled 'Specify the data source for the user authentication database' containing the text 'Provider=MSDASQL;DSN=EFT;UID=sa;PWD=sa;'. Below this text box is a checkbox labeled 'Encrypt user passwords stored in the database' which is checked. To the right of the checkbox is a dropdown menu labeled 'User list refresh interval:' with the selected option being 'Use server specified interval'. Below these elements is a 'Test Connection' button. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

- 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.



Override VFS Credentials

☐ Enable VFS credentials override

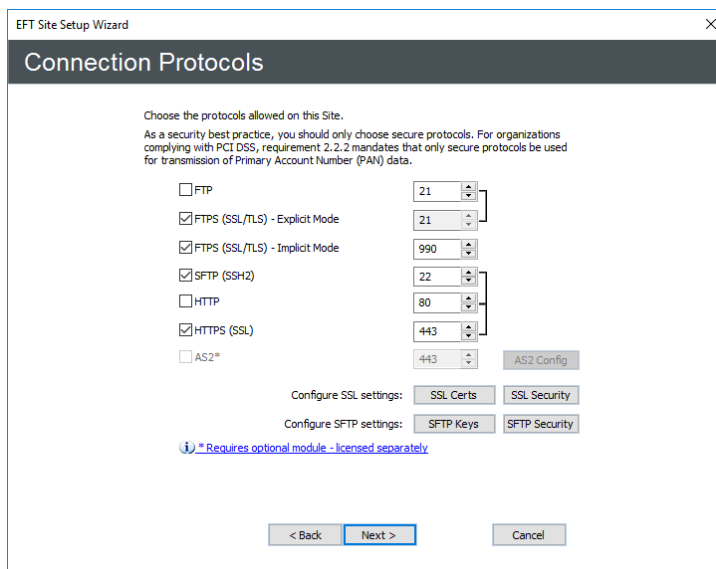
Login:

Password:

WARNING: If the option is enabled, the access may be lost to virtual shared folders, which had access via EFT Service account.

OK Cancel

- 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](#)

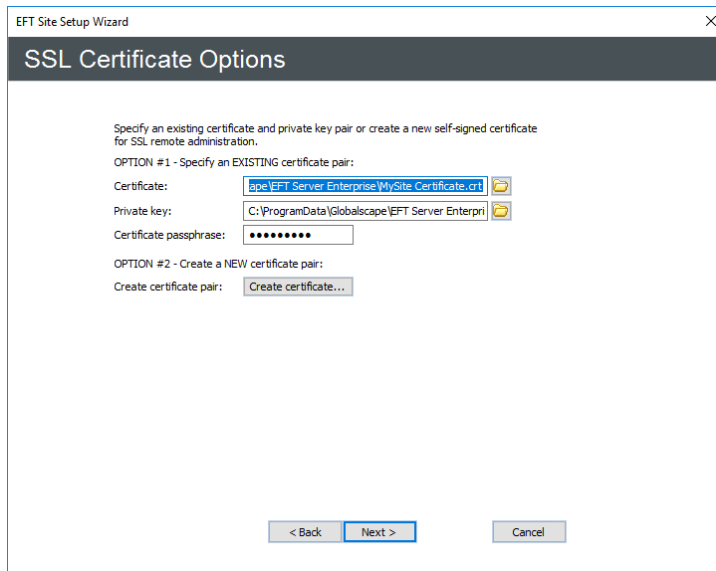
* Requires optional module - licensed separately

< 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 **.cer** 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 Database](#) for information regarding certificates.

19. Click **Next** to return to the **Protocols** page.
20. If you are using SSL, click **SSL options**:

EFT Site Setup Wizard

SSL Options

☒ Inherit from server settings

Allowed versions:

- ☒ TLSv1.2
- ☐ TLSv1.1
- ☐ TLSv1
- ☐ SSLv3

Allowed ciphers:

☒ Select algorithms and order by preference

Encryption [4/10]
 Message Authentication Code (MAC) [3/5]
 Key Exchange [2/7]
 Authentication [2/6]
 Cipher Suite Version [1/2]
 Export Status [1/1]

☐ Manually specify algorithms in order of preference (advanced)

EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3DES

Example: ALL:!LOW:!EXPORT:!MD5:@STRENGTH (see documentation)

Resulting cipher list (12 of 12 selected):

☒	Name	Version	Encryption	Mac	Key Exchange	Auth	Ex
☒	ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	AESGCM(256)	AEAD	ECDH	RSA	Nc
☒	ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	AESGCM(256)	AEAD	ECDH	ECDSA	Nc
☒	AES256-GCM-SHA384	TLSv1.2	AESGCM(256)	AEAD	RSA	RSA	Nc
☒	ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	AESGCM(128)	AEAD	ECDH	RSA	Nc

< Back Next > Cancel

- 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.
- TLSv1.2 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.

EFT Site Setup Wizard

SFTP Keys

SFTP private key name: Click the folder icon to import an existing key Create...

Passphrase:

< Back Next > Cancel

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.
 - Specify a name, location, format, and bit length of the key pair, and then click **Next**.
 - Specify and confirm the passphrase to encrypt the private key, and then click **Next**.
 - 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**.
 - 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.

EFT Site Setup Wizard

SFTP Options

☒ Inherit from server settings

SFTP (SSH2) Settings

Use encryption algorithms: Use message integrity algorithms: Use KEX ciphers:

☒ aes256-gcm@open	☒ hmac-sha2-512-etm@ope	☒ ecdh-sha2-nistp521
☒ aes256-ctr	☒ hmac-sha2-512	☒ ecdh-sha2-nistp384
☒ aes256-cbc	☒ hmac-sha2-256-etm@ope	☒ ecdh-sha2-nistp256
☒ rijndael-cbc@lysato	☒ hmac-sha2-256	☒ diffie-hellman-group18-sha512
☒ aes192-ctr	☒ hmac-sha1-etm@openssh	☒ diffie-hellman-group16-sha512
☒ aes192-cbc	☒ hmac-sha1	☒ diffie-hellman-group14-sha256
☒ aes128-gcm@open	☒ umac-64-etm@openssh.c	☒ diffie-hellman-group-exchange-sha256
☒ aes128-ctr	☒ umac-64@openssh.com	☒ diffie-hellman-group14-sha1
☒ aes128-cbc	☒ hmac-md5	☒ curve25519-sha256
☒ 3des-cbc	☒ hmac-sha1-96	☒ curve25519-sha256@libssh.org
☒ chacha20-poly1305	☒ hmac-md5-96	☒ sntrup4591761x25519-sha512@tinyssh.org
☒ cast128-ctr		☒ diffie-hellman-group-exchange-sha1

Optionally specify: protocol: software version: comments:

SSH-2.0- 8.1.0.0_openssh Globalscape

< Back Next > Cancel

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**.

- 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 wizard](#) to 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

When you run the [Site](#) creation wizard, you have the option to create a Site with advanced security options enabled and that can monitor, report, and/or warn when those settings are changed and can cause compliance violations. (Requires [RCM](#).)

Prerequisites:

- [Auditing and Reporting module](#) enabled
- [Regulatory Compliance Module](#) 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 high 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 [ARM](#) enabled?
- 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 an advanced 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.

EFT Site Setup Wizard

Site Security Policy

Choose the default security level for this Site:

☐ Default security settings (recommended)

☒ Strict security settings for compliance with PCI-DSS*

Note: Under "strict" security settings, certain preset security parameters, such as "Force user to reset password on initial login", require complex interaction during the setup process and upon initial log on.

If your company does not require PCI DSS compliance, then choose "Default Security Settings." You can manually enable advanced security options later, if needed.

* Requires optional module - licensed separately

< Back Next > Cancel

- Click **Strict security settings**, and then click **Next**. The **Site Label and Listening IP** page appears.

EFT Site Setup Wizard

Site Label and Listening IP

Configure a Site for servicing inbound connections.

To begin, provide a name for this Site. Create a unique, distinguishing label, as it is possible to have more than one Site running on the same physical server.

Site label:

If you have more than one IP address and plan on running multiple Sites on this server, specify the IP address this Site should listen on. Alternatively, choose **All Incoming** to service all IP addresses assigned to this computer.

Listening IPs:

< Back Next > Cancel

- 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.
- Next to the **Listening IPs** box, click **Configure**. The **Listening IP Settings** dialog box appears.

Listening IP Settings

Listening IPs:

- ☒ All Incoming (IPv4)
- ☐ All Incoming (IPv6)
- ☐ All Incoming (IPv4 and IPv6)
- ☐ 127.0.0.1
- ☐ 192.168.96.131
- ☐ ::1 (localhost)
- ☐ 2001:0:34f1:8072:3855:2cc4:3f57:9f7c
- ☐ fe80::3855:2cc4:3f57:9f7c%4 (link-local)
- ☐ fe80::3c63:7324:3026:90df%5 (link-local)

OK Cancel

- 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**.
- 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 Server 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 [RADIUS](#) or [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**, or the default of **None**. (**Common Access Card (CAC)** authentication is not allowed for high security-enabled Sites.)

- If **RADIUS** or **RSA SecurID** 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.)
- (Optional) Next to **Override VFS Credentials**, click **Configure**. Enable and provide login information, if needed. (Refer to [Override VFS Credentials](#) for details of this option.)

12. Click **Next**. The **Perimeter Network Security** page appears.

EFT Site Setup Wizard

Perimeter Network Security

Optional DMZ Gateway* configuration.

PCI DSS requirement 1.3.6 forbids system components that store cardholder data from residing in the DMZ. For security best practices, you should not store confidential data in your internal network zone.

Globalscape's DMZ Gateway facilitates secure connections between the DMZ and your internal network, *never* storing data in the DMZ. If you are using the DMZ Gateway, provide the listening IP address and port below:

☐ Connect this Site to EFT's DMZ Gateway

Host address(es): Port:

☒ Continue without configuring the DMZ Gateway

Note: Any explanation, justification, or compensating controls documented will be audited and included in EFT's PCI DSS compliance report.

[* DMZ Gateway licensed separately](#)

< Back Next > Cancel

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.

EFT Site Setup Wizard

Data Retention and Disposal

PCI DSS requirement 3.1 states: *Keep cardholder data storage to a minimum....* and 3.1.a states: *Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements.*

Optionally create a data retention and disposal policy using this wizard or create a customized data retention and disposal policy later using EFT's Timer Event Rule and Clean Up Action.

☐ Each day, delete files older than days matching these extensions from this folder: ☒ Include sub-folders

☒ Don't set a data retention and disposal policy

< Back Next > Cancel

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.

EFT Site Setup Wizard

Administrator Account Password Security

PCI DSS requirement 8.5 states: *Ensure proper user identification and authentication management for non-consumer users and administrators on all system components...*

PCI DSS violation: One or more strong password policy settings are disabled for administrator accounts.
Solution: Enable relevant password security settings

PCI DSS requirement section 8 outlines the following requirements:

- Force password reset upon first use
- Remove inactive accounts after at least 90 days
- Change password at least every 90 days
- Use complex passwords
- Limit repeated invalid log on attempts to no more than 6
- Set a lock-out duration or disable an account that exceeds the max log on attempt limit
- Idle admin sessions should timeout and require login credentials to continue

☒ Enable options identified above for all administrator accounts

☐ Continue without changing administrator account password security settings

< Back Next > Cancel

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.

The screenshot shows a window titled "EFT Site Setup Wizard" with a close button (X) in the top right corner. The main heading is "Daily PCI DSS Compliance Report". Below the heading, there is explanatory text: "PCI DSS requirement 10.6 relates to daily reviews of system component logs. EFT can assist you in this daily audit by generating a *PCI DSS compliance report* of EFT's security settings." and "Optionally generate and send a recurring daily PCI DSS compliance report to the administrator or designated user (below). You can always setup automated reports later using EFT's Scheduler (Timer) Event Rule and the Generate Report action." There are two radio button options: "Audit and send daily report" (which is selected) and "Do not generate daily report". The "Audit and send daily report" option has a text input field labeled "Recipient e-mail:". The "Do not generate daily report" option has a text input field labeled "Provide justification and describe the compensating controls". At the bottom, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

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.

EFT Site Setup Wizard

Data Sanitization

PCI DSS 9.8.2 requires wiping of deleted cardholder data so that it cannot be reconstructed.
 Solution: EFT supports data wiping techniques of varying levels of efficiency vs. speed tradeoffs. Select a wiping method below (applies to all EFT delete operations) or choose the Windows default (no wipe).

☐ Enable data wiping
 Data sanitization method: Pseudorandom data (medium)

☒ Windows default (no wipe)
 Provide justification and describe the compensating controls

< Back Next > Cancel

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.

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

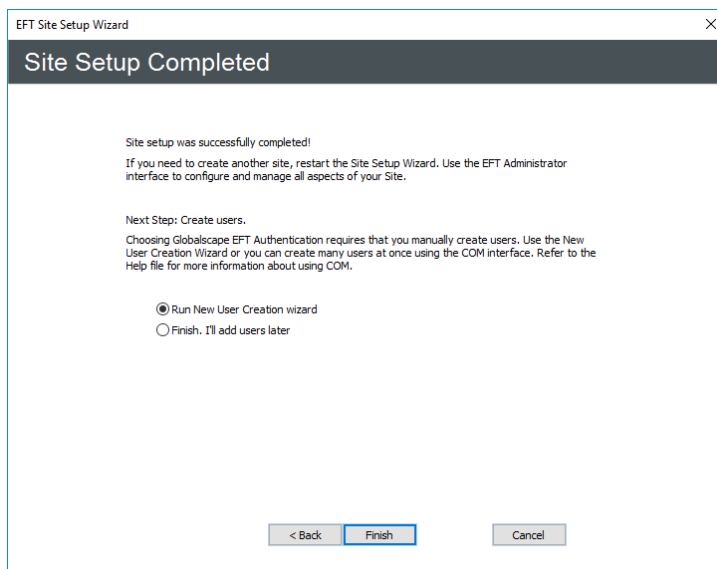
Configure SFTP settings: SFTP Keys SFTP Options

* Requires optional module - licensed separately

< Back Next > Cancel

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

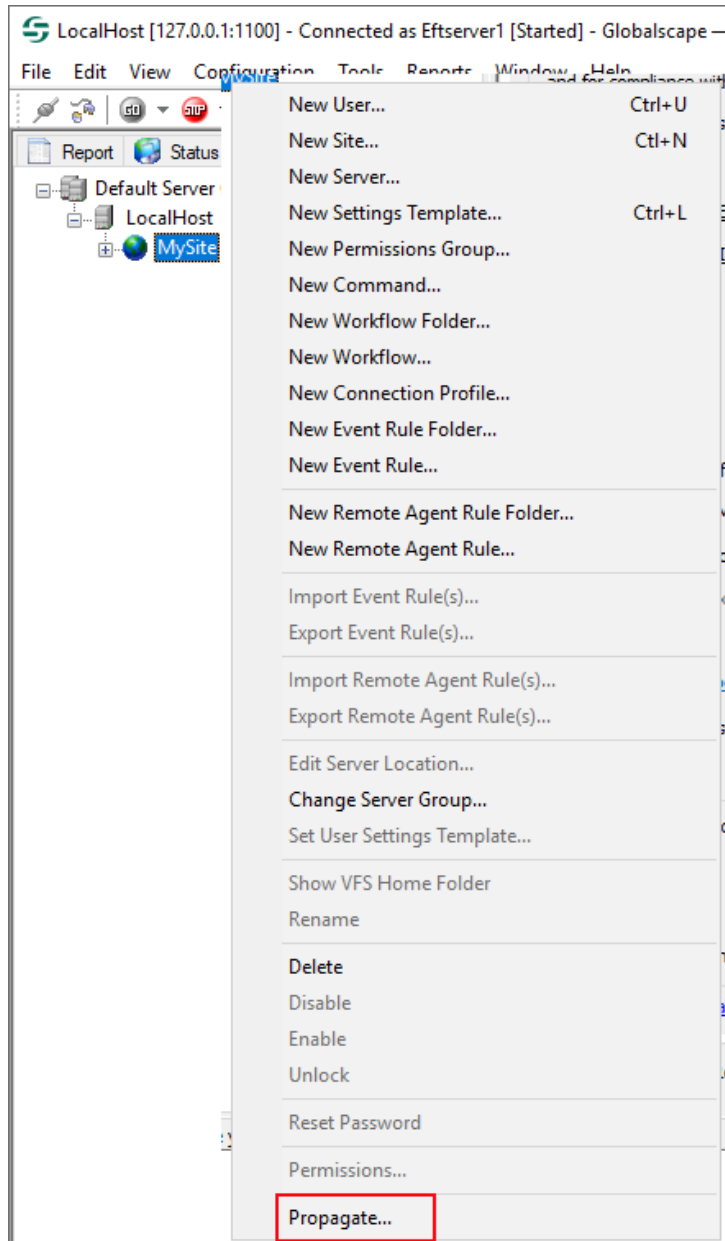
For disaster recovery, some customers need to perform a unidirectional sync across settings from a live EFT site to another so that a backup system is available.

To propagate an EFT Site

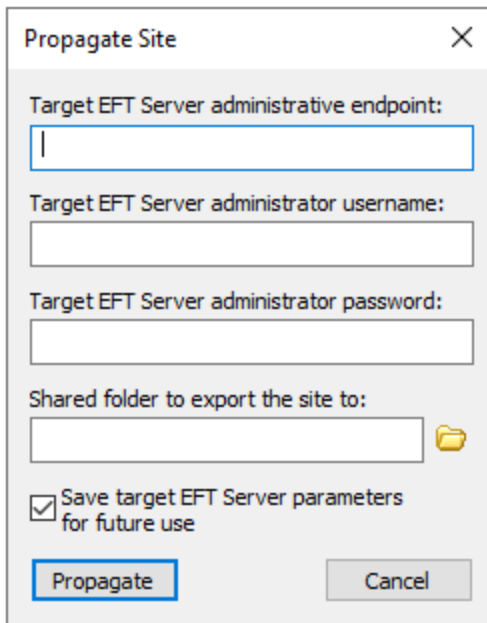
- Internally, propagation is performed via target server's REST Administrator interface, so target server must have Web-admin enabled for the feature to work.
- The administrator must be at least a Site-level Administrator.
- Administrator account must have **Programmatic API Policy** enabled.
- The 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.

The screenshot shows the 'Administration' tab of the EFT Server Administration console. The 'Server Administration Connectivity' section includes options for 'Server administrator listening IP' (set to 'All Incoming (IPv4)'), 'Port' (1100), and 'Allow remote administration' (checked). Under 'Allow remote administration', 'Enable REST API / web admin' is checked, 'REST API / web admin port' is 4450, and 'Require SSL for remote administration' is checked. The 'Administrator Access and Permissions' section shows 'Admin account names' with 'Eftserver1' and 'Local computer\Administrators'. The 'Selected account permissions policy' is 'Server Admin(full control)'. Under 'Optional permissions', 'Run & Edit Reports', 'Manage personal data', and 'COM (programmatic control)' are checked. The 'Assigned to this server' section is empty. At the bottom, the 'Programmatic API Policy' dropdown is set to 'server_full_access'.

- 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**.



The dialog box titled "Propagate Site" contains the following fields and controls:

- Target EFT Server administrative endpoint:** A text input field.
- Target EFT Server administrator username:** A text input field.
- Target EFT Server administrator password:** A text input field.
- Shared folder to export the site to:** A text input field with a folder icon to its right.
- ☒ **Save target EFT Server parameters for future use**
- Buttons:** "Propagate" and "Cancel".

- **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**.

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.

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 FTP/S Config
☐ FTPS (SSL / TLS) - Explicit mode* 21
☐ FTPS (SSL / TLS) - Implicit mode* 990
☐ SFTP (SSH2)* 22 SFTP Config
☐ HTTP* 80 Domain: localhost
☒ HTTPS (SSL)* 443

☐ 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

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 **AS2** access, 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.

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)

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.

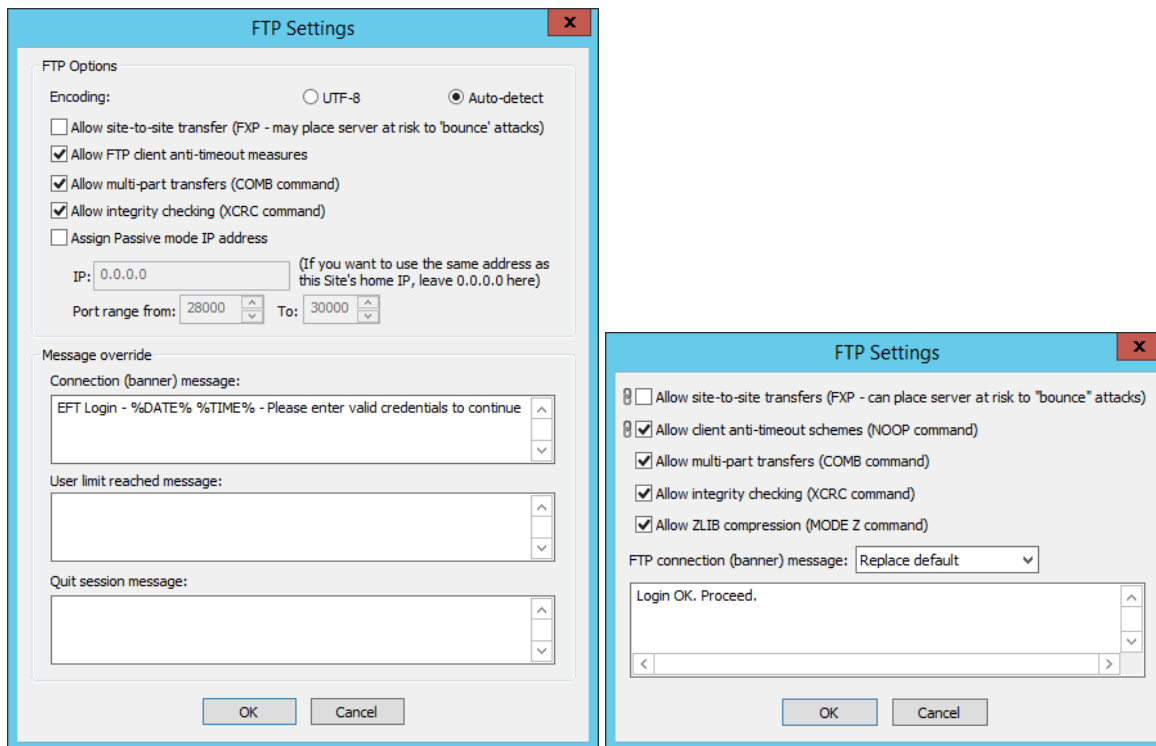
You can configure FTP connections to the Site on the Site's **Connections** tab. You can enable or disable FTP transfers at the Site, Setting Template, or per user.

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.



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 been 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`:

```

[4/12/2010 3:27:13 PM] 150 Opening ASCII mode data connection for file list.
[4/12/2010 3:27:13 PM] 226 Transfer complete. 542 bytes transferred. 542 bps.
STATUS:> [4/12/2010 3:27:13 PM] Directory listing completed.
COMMAND:> [4/12/2010 3:28:36 PM] SYST
[4/12/2010 3:28:36 PM] 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.aspx> for 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

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.

The screenshot shows the 'Connections' tab in the administration interface. It is divided into two main sections: 'Listener Settings' and 'Network Usage and Security Settings'.

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:** A dropdown menu is set to 'All Incoming (IPv4)'.
- Protocols and Ports:**
 - ☐ FTP: Port 21
 - ☐ FTPS (SSL / TLS) - Explicit mode*: Port 21
 - ☐ FTPS (SSL / TLS) - Implicit mode*: Port 990
 - ☐ SFTP (SSH2)*: Port 22
 - ☐ HTTP*: Port 80
 - ☒ HTTPS (SSL)*: Port 443
- Domain:** A text field containing 'localhost'.
- AS2***: Includes 'AS2 Config' buttons and instructions: '- Use yourdomain/as2 for AS2 account management' and '- Use yourdomain for inbound AS2 transactions'.
- Require additional factor for HTTP/S auth:***: A dropdown menu set to 'OTP - Email delivery'.
- SMS Config**: A button.
- ☒ Allow Globalscape Mobile Transfer Client (MTC) over HTTPS: Includes a 'Configure' button.
- ☐ 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:** Includes a 'Configure' button and the text '(Applies to HTTPS, FTPS, Web Services and AS2)'.
- SSL security settings:** Includes a 'Configure' button.

Network Usage and Security Settings:

- Connection limits:** Includes a 'Configure' button.
- IP access/ban list:** Includes a 'Configure' button.
- Denial of Service settings:** Includes a 'Configure' button.

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](#).

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.

- 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.

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.

The screenshot shows the 'Connections' tab in the EFT administration interface. The 'Listener Settings' section is active, displaying a list of protocols and their corresponding ports. The 'Enable HSTS' checkbox is checked. The 'Listening IP addresses' field is set to 'All Incoming (IPv4)'. The 'Domain' field is set to 'localhost'. The 'SSL certificate settings' and 'SSL security settings' sections are also visible.

Protocol	Port	Configuration
☐ FTP	21	FTP/S Config
☐ FTPS (SSL / TLS) - Explicit mode*	21	
☐ FTPS (SSL / TLS) - Implicit mode*	990	
☐ SFTP (SSH2)*	22	SFTP Config
☐ HTTP*	80	Domain: localhost
☒ HTTPS (SSL)*	443	
☐ AS2*		AS2 Config
☐ 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

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.json](#) file 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](#).)

`\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.

General Connections **Security**

Specify the settings for this user.

Protocols

☐ FTP FTP configuration options: [FTP Config](#)

☐ FTPS (SSL/TLS)* SSL authentication options: [SSL Auth](#)

☐ SFTP (SSH2)* SFTP authentication options: [SFTP Auth](#)

☐ HTTP*

☒ **HTTPS***

☒ Allow Web Transfer Client (WTC) over HTTP/S

☒ Allow secure folder sharing*

☒ Allow secure file sending (web and Outlook add-in)*

☐ AS2 inbound* [AS2 Inbound](#)

☐ AS2 outbound* [AS2 Outbound](#)

Network Usage & Limits

Connection limits: [Configure](#)

Transfer limits: [Configure](#)

IP access/ban list: [Configure](#)

[* Requires optional module - licensed separately](#)

- In the **Protocols** area, select the **Allow Web Transfer Client over HTTP/S** check box.

HTTPS must also be enabled.

- 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.)

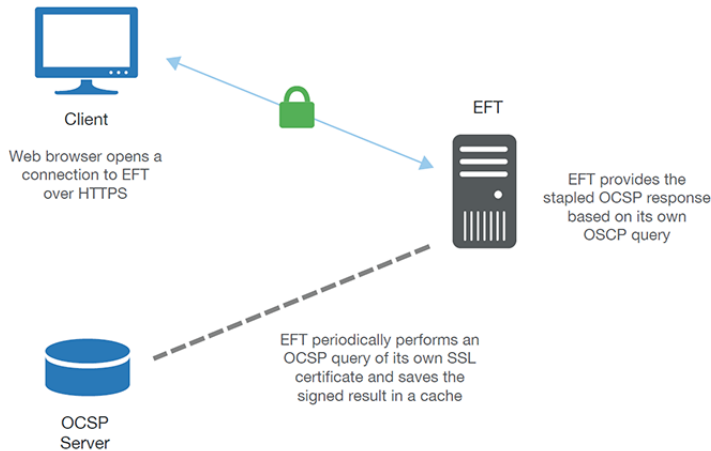
Refer to <https://lessonsintech.wordpress.com/2016/02/10/configure-ocsp-stapling-f5-ltm/> and https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ssl-administration-11-6-0/4.html for more information.

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.

- <https://kb.globalscape.com/KnowledgebaseArticle11362.aspx> Adjust for time drift (skew) between the CA and EFT for OCSP requests
- <https://kb.globalscape.com/KnowledgebaseArticle11363.aspx> Specify a maximum allowable age for OCSP stapling responses
- <https://kb.globalscape.com/KnowledgebaseArticle11364.aspx> Override the OCSP responder URI specified in the certificate's AIA extension

- <https://kb.globalscape.com/KnowledgebaseArticle11365.aspx> Enable the OCSP response
- <https://kb.globalscape.com/KnowledgebaseArticle11366.aspx> OCSP Stapling cache timeout

Redirecting HTTP to HTTPS

(Requires the HTTP/S module; redirect not available in Globalscape EFT) 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.

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:

☐ FTP

☐ FTPS (SSL / TLS) - Explicit mode*

☐ FTPS (SSL / TLS) - Implicit mode*

☐ SFTP (SSH2)*

☐ HTTP* Domain:

☒ HTTPS (SSL)*

☐ AS2* - Use yourdomain/as2 for AS2 account management
- Use yourdomain for inbound AS2 transactions

☐ Require additional factor for HTTP/S auth:*

☒ Allow Globalscape Mobile Transfer Client (MTC) over HTTPS

☐ 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: (Applies to HTTPS, FTPS, Web Services and AS2)

SSL security settings:

Network Usage and Security Settings

Connection limits:

IP access/ban list:

Denial of Service settings:

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.

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.

The screenshot shows the 'Connections' tab in the EFT Administration interface. The 'Listener Settings' section is active, displaying options for listening IP addresses and protocols. The 'Listening IP addresses' dropdown is set to 'All Incoming (IPv4)'. The 'Protocols' section includes checkboxes for FTP, FTPS (SSL/TLS) - Explicit mode*, FTPS (SSL/TLS) - Implicit mode*, SFTP (SSH2)*, HTTP*, and HTTPS (SSL)*. The 'HTTPS (SSL)*' checkbox is checked, and its port is set to 443. The 'Domain' is set to 'localhost'. The 'AS2*' checkbox is unchecked, and the 'AS2 Config' button is visible. The 'Require additional factor for HTTP/S auth:*' dropdown is set to 'OTP - Email delivery'. The 'Allow Globalscape Mobile Transfer Client (MTC) over HTTPS' checkbox is checked. The 'Event Rule invoke over WS/SOAP (uses HTTPS port)*' checkbox is unchecked. The 'Redirect all plaintext HTTP traffic to HTTPS*' checkbox is unchecked. The 'Enable HSTS' checkbox is checked. The 'Enable Proxy Protocol for all protocols enabled on this Site' checkbox is unchecked. The 'SSL certificate settings' and 'SSL security settings' buttons are visible. The 'Network Usage and Security Settings' section includes buttons for 'Connection limits:', 'IP access/ban list:', and 'Denial of Service settings:'.

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.

- Click **Apply** to save the changes on EFT.

To use the scripts for testing Web Service

- **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

- 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!

- 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 account](#) login credentials, not USER credentials!

3. The EFTWebService interface appears.

The screenshot shows the EFTWebService interface. At the top, it says "EFTWebService". Below that, it states: "The following operations are supported. For a formal definition, please review the [Service Description](#)." There is a bullet point for [InvokeEventRule](#) with the description: "Invoke the named Event Rule on the GlobalSCAPE Enhanced File Transfer (EFT) Server. The context values are a semicolon separated list of NAME=VALUE pairs to fill out context variables for the rule execution."

4. Click **InvokeEventRule**. Another Web page, **/WebService/InvokeEventRule**, displays a form for invoking an Event Rule.

The screenshot shows the EFTWebService InvokeEventRule form. It has a title "EFTWebService" and a subtitle "InvokeEventRule". Below the subtitle, it says: "Invoke the named Event Rule on the GlobalSCAPE Enhanced File Transfer (EFT) Server. The context values are a semicolon separated list of NAME=VALUE pairs to fill out context variables for the rule execution." There is a "Test" section with the instruction: "To test the operation using the HTTP POST protocol, click the 'Invoke' button." Below this is a form with two input fields: "EventRuleName:" and "EventParams:". There is an "Invoke" button at the bottom right.

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.)

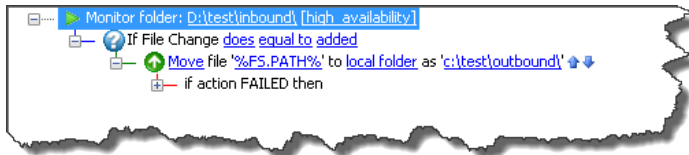
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<int xmlns="https://localhost">1</int>
```

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



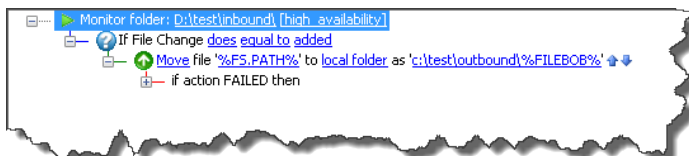
To test the operation using the HTTP POST protocol, click the 'Invoke' button.

Parameter	Value
EventRuleName:	ProcessTestFileName
EventParams:	FS.PATH=C:\test\inbound\test.txt;FS.MONITOR_OPERATION=added

Invoke

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=string
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=ProcessTest
FileName&EventParams=FS.PATH=C:\test\inbound\test.txt;FS.MONITOR_
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
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

Method	EFT Support
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: <pre>>>Request MKCOL /webdisc/xfiles/ HTTP/1.1 Host: www.example.com >>Response HTTP/1.1 201 Created</pre> 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.
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.

Method	Description, Examples, and Error Codes
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. <pre>>>Request DELETE /container/ HTTP/1.1 Host: www.example.com</pre>
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. <pre>Destination = "Destination" ":" Simple-ref</pre>

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 Outgoing Ciphers and Advanced Properties

[Advanced Properties](#) are 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_OPENSSSH_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_OPENSSSH_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_OPENSSSH_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

SFTP Logging

In the [logging.cfg](#) file, you can configure logging for SFTP transfers. In the [ARM schema](#), the table **tbl_NegotiatedCiphersSSH** is associated with **tbl_Authentications** and **tbl_Actions**, which tracks the negotiated cipher set for successful SFTP client/server authentications.

- Setting the following [advanced properties](#) to **true** will improve the log performance: **EnableXferLog** (enable transfer logs) and **CloseFinishedItemLog** (false = enabled/default. By default, successful logs are removed.)
- You can see negotiated ciphers in the EFT client log files, for troubleshooting purposes.

To configure logging for SFTP transfers

1. Open logging.cfg in a text editor, such as Notepad.
2. Find this line:

```
#log4cplus.logger.SFTP=TRACE
```

3. Delete the # from the front of the line to enable the logger.
4. Leave as TRACE or change to DEBUG for troubleshooting.

If you change it to DEBUG, be sure to change it back to TRACE and/or add the # to the front to comment out (disable) that log to avoid creating unnecessarily large log files.

Note that there are differences in how the logs are displayed depending on whether you are using SFTP.DLL or SFTP2.DLL.

When using the SFTP2.dll, the logs at the KEX section are in ASCII format:

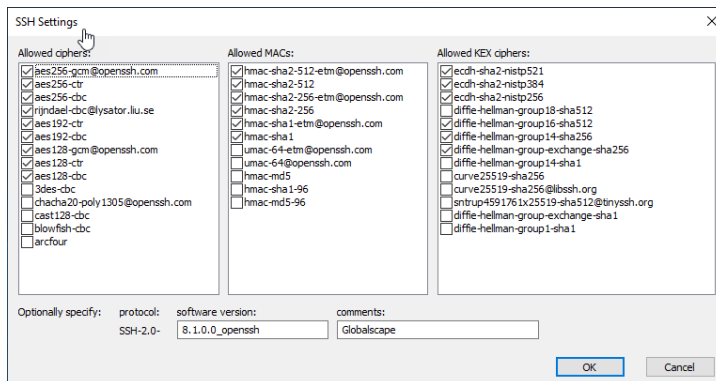
```
08-03-18 07:03:08,947 [3028] INFO Events.Server.MySite.Timer_SFTP_download <Timer: Timer SFTP download; Timer: Timer SFTP download> - Starting Timer for rule
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] id exchange: client protocol version 2.0; client software version clientSftp
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] no match: clientSftp
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] kex: start
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] rekey after 1073741824 bytes, 3600 seconds
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] kex names ok: [diffie-hellman-group16-sha512,diffie-hellman-group14-sha256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1]
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] send packet: type 20
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] SSH2_MSG_KEXINIT sent
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] receive packet: type 20
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] SSH2_MSG_KEXINIT received
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] local server KEXINIT proposal
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] kex names follow: 0
```

[illegible]

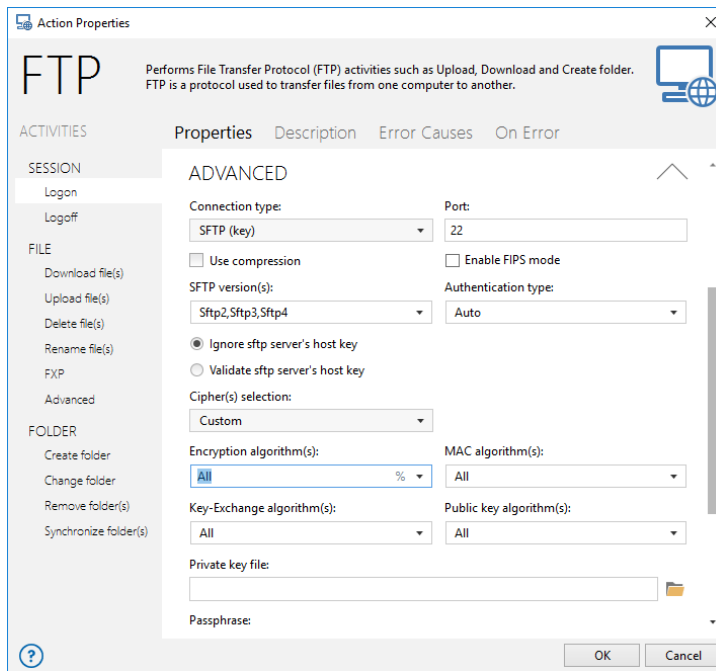
SFTP Encryption Algorithms

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.

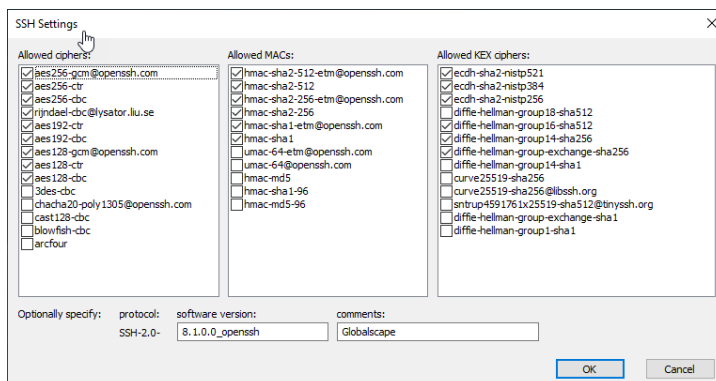


Enabling SFTP (SSH) on the Server

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.

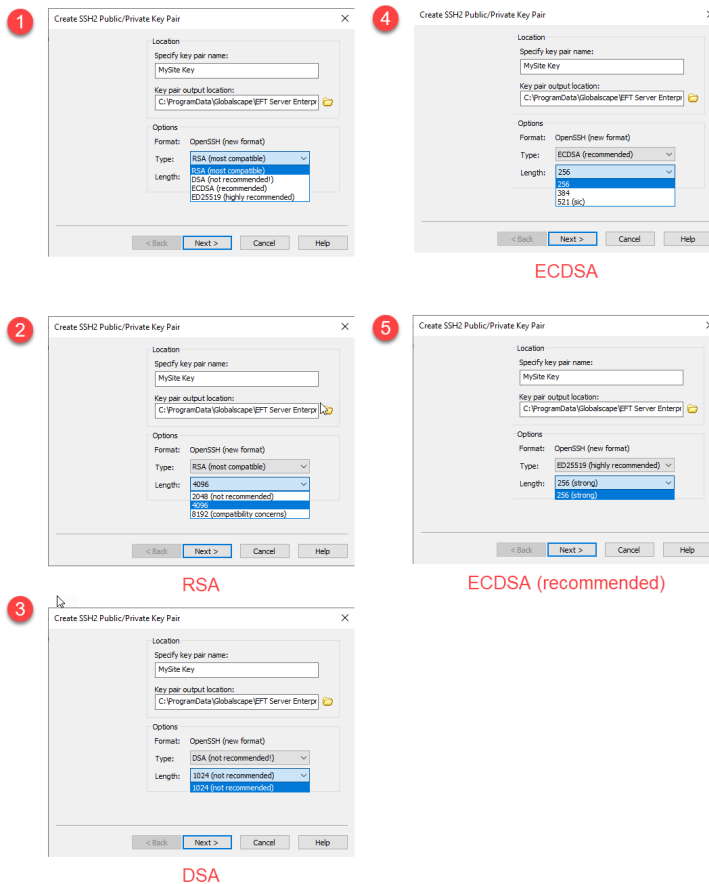
For the KEX ciphers, there are a few configuration changes to note:

- 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.

- Click **Next**. The password page of the wizard appears.

Enter the passphrase to encrypt the private key:

Passphrase:

Confirm

- 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)

- Click **Next**.

Please choose the key's purpose below. You can optionally create or replace the currently assigned host keypair, create a keypair intended for assignment to a given user account, or just create the keypair for later use.

☒ Create as host key for: MySite
Keypair will be copied to the key manager and assigned to the Site name above

☐ Create as client keypair
Public key will be copied to the key manager

☐ Just create keypair
Keypair will be created on disk only

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 saved in **C:\ProgramData\Globalscape\EFT Server**.

PowerShell Example

Refer to the [COM API help](#) for details of using the [CreatSSHKeyPair](#) method.

In PowerShell, use the following example:

```
$privateKeyFile = New-Object Object
$publicKeyFile = New-Object Object
#define VariantWrapper for variables to be passed as VARIANT
$wrappedPublic = New-Object
Runtime.InteropServices.Marshal::VariantWrapper($publicKeyFile)
$wrappedPrivate = New-Object
Runtime.InteropServices.Marshal::VariantWrapper($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_OPENSSSH_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_OPENSSSH_COM to false
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

Advanced Property	Description
SFTP2_HMAC_SHA2_256_ETM_AT_OPENSSSH_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_OPENSSSH_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_OPENSSSH_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_OPENSSSH_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
SFTP2_UMAC_64_ETM_AT_OPENSSSH_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_OPENSSSH_COM to false

Advanced Property	Description
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

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 [import](#) an SFTP key defined on the Site. Be sure to select **Create as host key for: <site_name>** before you click **Finish**.

Please choose the key's purpose below. You can optionally create or replace the currently assigned host keypair, create a keypair intended for assignment to a given user account, or just create the keypair for later use.

☒ Create as host key for: MySite
Keypair will be copied to the key manager and assigned to the Site name above

☐ Create as client keypair
Public key will be copied to the key manager

☐ Just create keypair
Keypair will be created on disk only

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.

SFTP Settings

Transfer Options

Filename encoding: ☒ UTF-8 ☐ ASCII

Security Options

SFTP private key name:

Public key blob:

Create new key pair:

Extract and export public key from private key:

Manage client (end user) public keys:

Advanced Security Options

Allowed ciphers:

- ☒ 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
- ☒ chacha20-poly1305@openssh.com
- ☒ cast128-cbc

Allowed MACs:

- ☒ 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

Allowed KEX ciphers:

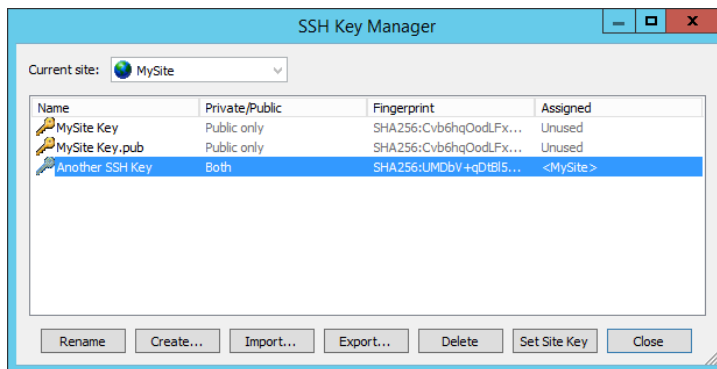
- ☒ ecdh-sha2-nistp521
- ☒ ecdh-sha2-nistp384
- ☒ ecdh-sha2-nistp256
- ☒ diffie-hellman-group18-sha512
- ☒ diffie-hellman-group16-sha512
- ☒ diffie-hellman-group14-sha256
- ☒ diffie-hellman-group-exchange-sha256
- ☒ diffie-hellman-group14-sha1
- ☒ curve25519-sha256
- ☒ curve25519-sha256@libssh.org
- ☒ sntrup4591761x25519-sha512@tinyssh.org
- ☒ diffie-hellman-group-exchange-sha1

Optional specify: protocol: software version: comments:

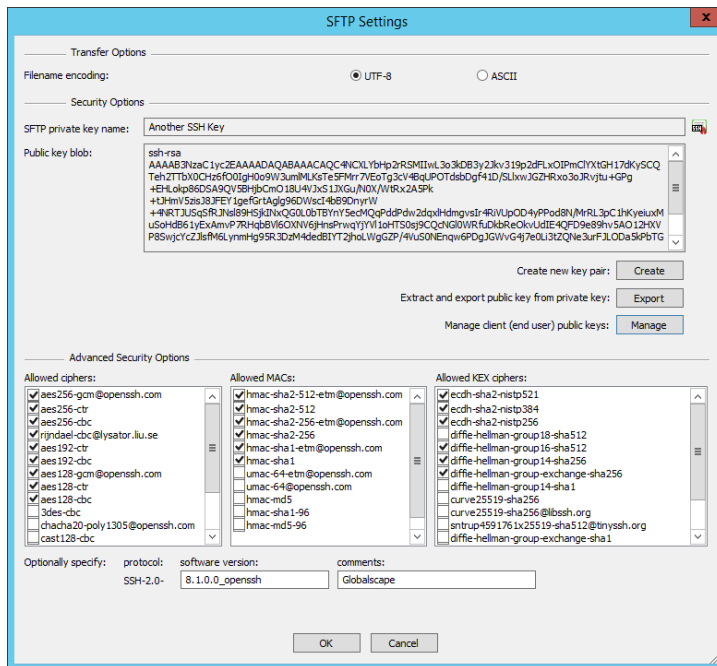
SSH-2.0- 8.1.0.0_openssh Globalscape

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.



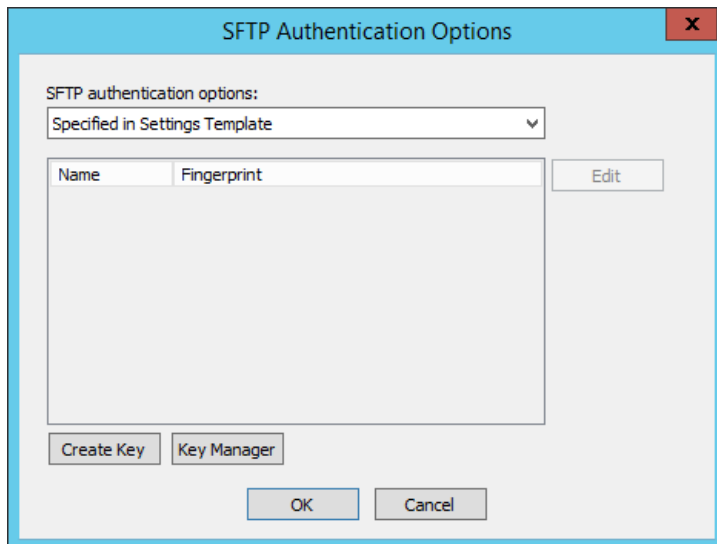
7. In the **Filename encoding** area, click **UTF-8** or **ASCII**.
 - **UTF-8**—For Unicode-only transfers
 - **ASCII**—Detects whether to proceed in ASCII mode or switch to UTF-8 mode for the transmission and receipt of path names and other strings communicated between client and server.
8. Click **OK** to close the dialog box.
9. Click **Apply** to save the changes.

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 [Connections](#) tab.
4. In the **Protocols** area, select the **SFTP (SSH2)** check box, then click **SFTP Auth**. The **SFTP Authentication Options** dialog box appears.

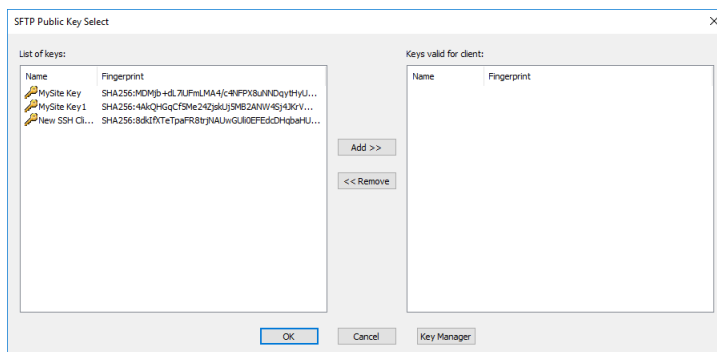


5. In the **SFTP authentication options** list, specify whether user are to connect using **Password only**, **Public key only**, **Public Key & Password**, or **Public key or Password**.

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.

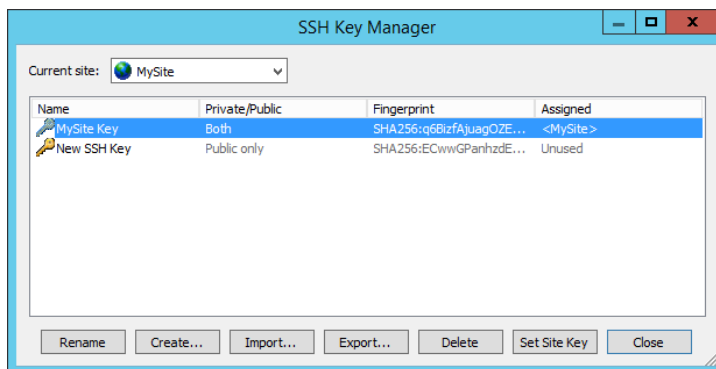
8. Click **OK** to close the **SFTP Public Key Select** dialog box. The selected key(s) appear in the **Authentication key list**.
9. Click **OK** to close the **SFTP Authentication Options** dialog box.
10. Click **Apply** to save the changes on EFT.

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.

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 [import](#) an 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.

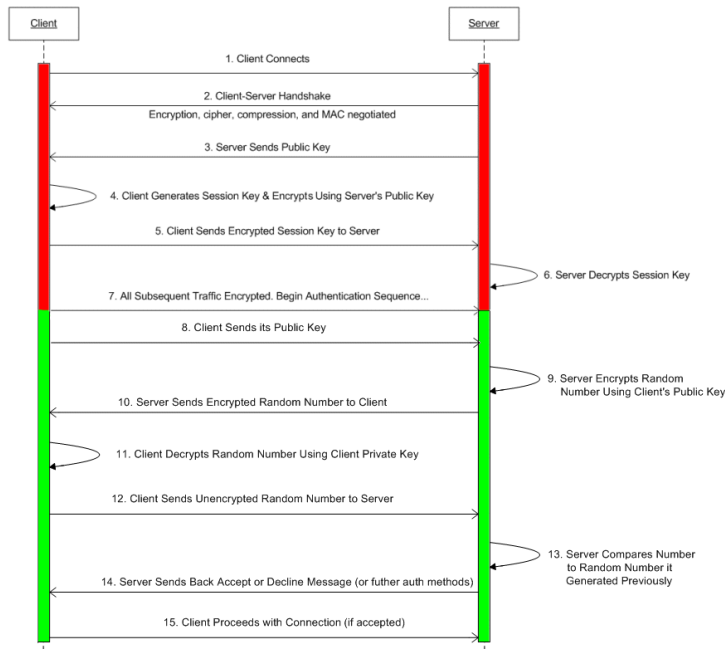
For more information about modifying the SFTP identification string, refer to <http://www.ietf.org/rfc/rfc4253.txt> section 4.2.

SFTP Key Support

(Requires the SFTP module) EFT supports the following actions for SFTP key support:

- 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.

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-exchange-sha256
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1

The screenshot shows the 'Advanced Security Options' dialog box with three columns of settings:

Allowed ciphers:	Allowed MACs:	Allowed KEX ciphers:
☒ aes256-cbc	☒ hmac-sha2-512	☒ diffie-hellman-group16-sha512
☒ aes256-ctr	☒ hmac-sha2-256	☒ diffie-hellman-group14-sha256
☒ 3des-cbc	☒ hmac-sha1	☒ diffie-hellman-group-exchange-sha256
☒ aes128-cbc	☐ hmac-md5	☐ diffie-hellman-group-exchange-sha1
☒ aes128-ctr	☐ hmac-sha1-96	☒ diffie-hellman-group14-sha1
	☐ hmac-md5-96	☐ diffie-hellman-group1-sha1

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.

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/GETBbzP83LOcekM02aRjo55Ar07gPPVvCXbrirJu9pkm4AC4BBre5xSLS
7soyzwbigFruM8G63jSXqpHqJ/ooil68sKMC2b0Ncsi+JlTfNYlDXJVLKEeZgZOInQyMmt
isaDTUQWTivlsnAizf4iIYENuAkGYGNCL77u5Y5VOu5eQipvFajTnps9QvUx/zdSFYn9e2
sulWM3Bxc/S4IJ67JWHVRpfJxGi3hinRBH8WQdXuUwdJJTiJHKPyYrrM7Q6Xq4TOMFtcRu
LDC6u3BXM1L0gBvHPNOnD5l2Lp5EjUkQ9CBf2j4A4gfH+iWQZyk08esAG/iwArAVxkl368
+dkbMWOXL8BN4x5zYgdzoeypQZZ2RKH780MCTSo4WQ19DP8pw+9q3bSFC9H3xYAxrKAJNW
jeTUJOTrTe+mWXXU770gYyQTxa2ycnYrlZucn1S3vsvn6eq7NZZ8NRbyv1n15Ocg+nHK4f
uKOrwPhU3NbKQwtjb0WsxxlgAmQqIOLTPAdsrAauPxC7TPYA5qQVCphvimKuhQM/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

AAAAB3NzaC1yc2EAAAABIwAAAQEAwrr66r8n6B8Y0zMF3dOpXEapIQD9DiYQ6D6/zwor9o
39jSkHNIEMMER/GETBbzP83LOcekm02aRjo55Ar07gPPVvCXbrirJu9pkm4AC4BBre5xSLS
7soyZWbigFruM8G63jSXqpHqJ/ooi168sKMC2b0Ncsi+JlTfNYlDXJVLKEeZgZOInQyMmt
isaDTUQWTiv1snAizf4iIYENuAkGYGNCL77u5Y5VOu5eQipvFajTnps9QvUx/zdSFYn9e2
sulWM3Bxc/S4IJ67JWHVRpfJxGi3hinRBH8WQdXuUwdJJTiJHKPyYrrM7Q6Xq4TOMFtcRu
LDC6u3BXM1L0gBvHPNOnD5l2Lp5EjUkQ9CBf2j4A4gfH+iWQZyk08esAG/iwArAVxkl368
+dkbMWOXL8BN4x5zYgdzoeypQZZ2RKH780MCTSo4WQ19DP8pw+9q3bSFC9H3xYAxrKAJNW
jeTUJOTrTe+mWXXU770gYyQTxa2ycnYrlZucn1S3vsvn6eq7NZZ8NRbyv1n150cg+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:

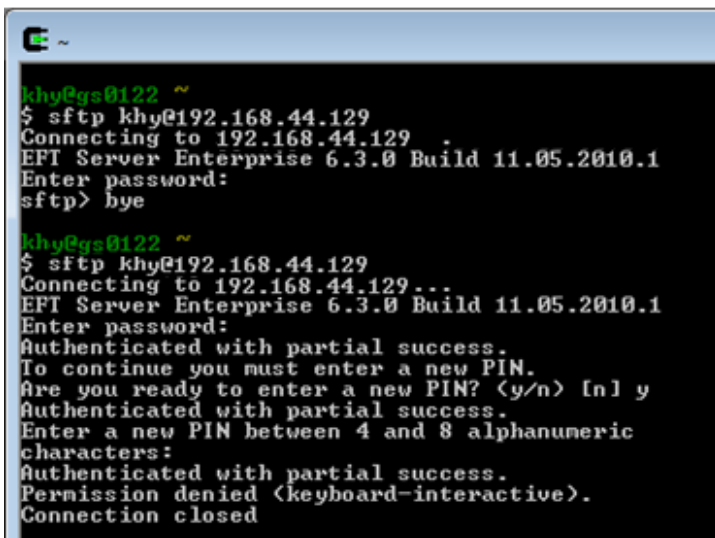
4096 18:9f:7d:8f:e0:ab:13:56:b7:49:89:b3:07:93:9f:da id_rsa.pub

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.



```

khy@qs0122 ~
$ sftp khy@192.168.44.129
Connecting to 192.168.44.129 .
EFT Server Enterprise 6.3.0 Build 11.05.2010.1
Enter password:
sftp> bye

khy@qs0122 ~
$ sftp khy@192.168.44.129
Connecting to 192.168.44.129...
EFT Server Enterprise 6.3.0 Build 11.05.2010.1
Enter password:
Authenticated with partial success.
To continue you must enter a new PIN.
Are you ready to enter a new PIN? <y/n> [n] y
Authenticated with partial success.
Enter a new PIN between 4 and 8 alphanumeric
characters:
Authenticated with partial success.
Permission denied (keyboard-interactive).
Connection closed

```

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/.

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.

AS2

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.

Introduction to AS2

(Requires AS2 module) 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 sent 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 acknowledgements 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, acknowledgements, 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](#).

How EFT Supports AS2

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:

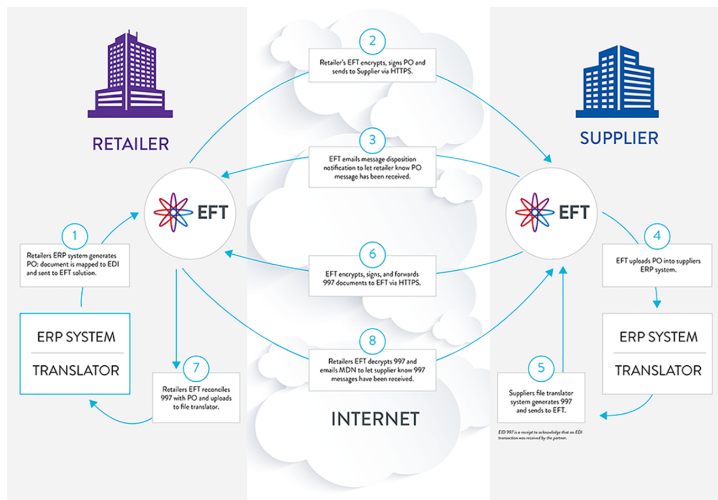
- An [On File Upload](#) Event occurs for each file uploaded in an MA transaction.
- An [AS2 Inbound Transaction Succeeded](#) Event occurs just once per single file or MA transaction **after** all files are received and the MDN (if requested) is successfully sent.
- An [AS2 Inbound Transaction Failed](#) 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

Installing and Activating the AS2 Module

AS2 is available to evaluate during the EFT trial.

Prerequisites for Using the AS2 Module

- EFT
- 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.
- You must have the [Auditing and Reporting module](#) installed. (The ARM trial is installed when you install EFT.)

If the AS2 module is not activated, the following events occur when the AS2 module trial has expired:

- All incoming AS2 connections are rejected.
- EFT audits the failure in the ARM database as "AS2 evaluation license expired."
- Any Event Rule that contains an **AS2 Send File to host** Action 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 unavailable.
- The **AS2 Send File to host** Event Rule Action is no longer available for Event Rules.
- EFT writes a message to the Windows Application Event Log.

AS2 Authentication

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 190*](#) 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 363](#), [Setting Maximum Transfer Size on page 424](#) to a reasonable level, or select the [Enabling SSL on the Site on page 180](#) 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

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, 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
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.

Enabling the AS2 Inbound Listener Service

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.

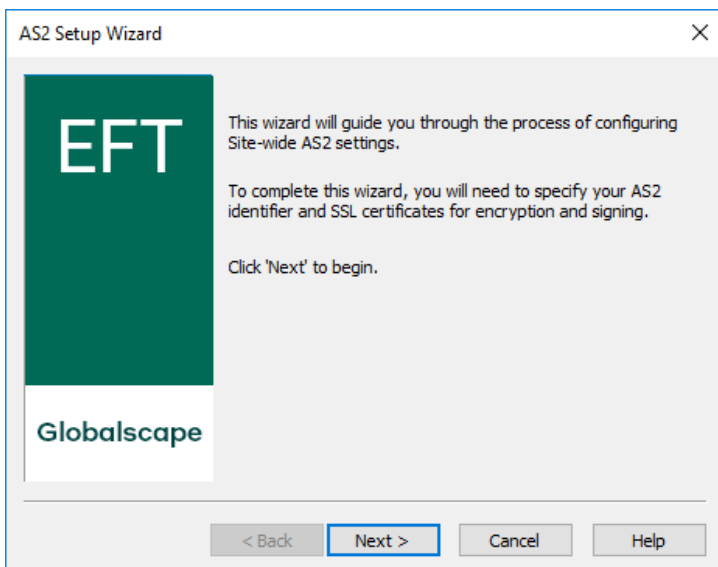
- **SSL certificate pair path** for signing and encrypting AS2 messages. If the SSL certificate pair does not already exist, you are given the option to create one from within the **AS2 Server Configuration** dialog box.

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.)

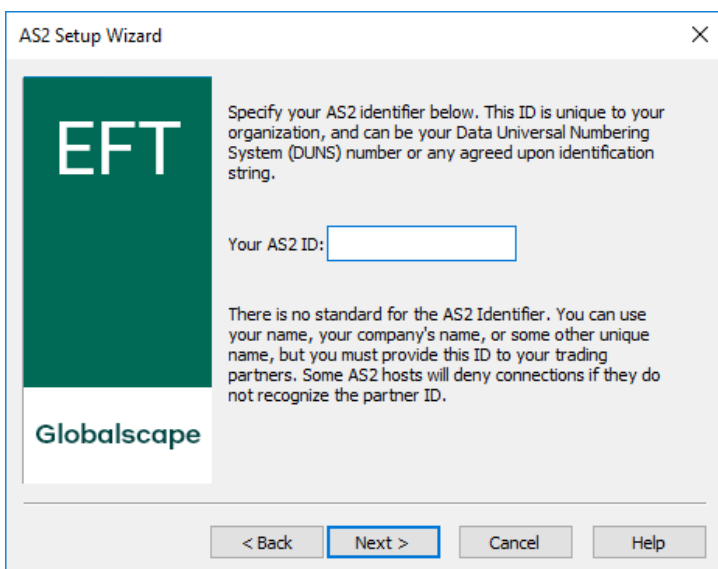
- EFT and the ARM module must be activated (or trial mode), and the ARM database must be configured.

To enable the AS2 inbound listener service

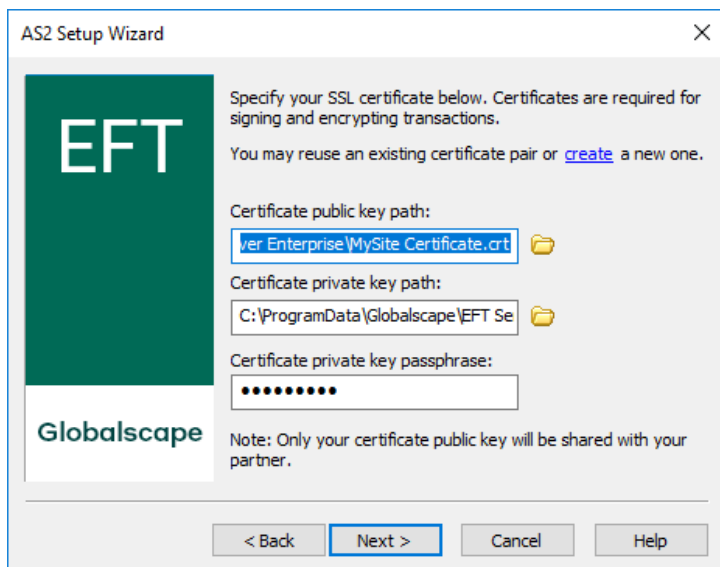
1. In the administration interface, [connect to EFT](#) and click the **Server** tab.
2. On the **Server** tab, click the Site that you want to configure.
3. In the right pane, click the **Connections** tab.
4. Select the **AS2** check box, and then click **AS2 Config**. The **AS2 Setup Wizard** appears.



5. Read the **Welcome** page, and then click **Next**. The **AS2 identifier** page appears.

The image shows the 'AS2 Setup Wizard' window at the 'AS2 Identifier' step. The left sidebar is identical to the previous screen. The main area contains the following text: 'Specify your AS2 identifier below. This ID is unique to your organization, and can be your Data Universal Numbering System (DUNS) number or any agreed upon identification string.', a text input field labeled 'Your AS2 ID:', and a paragraph: 'There is no standard for the AS2 Identifier. You can use your name, your company's name, or some other unique name, but you must provide this ID to your trading partners. Some AS2 hosts will deny connections if they do not recognize the partner ID.' At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

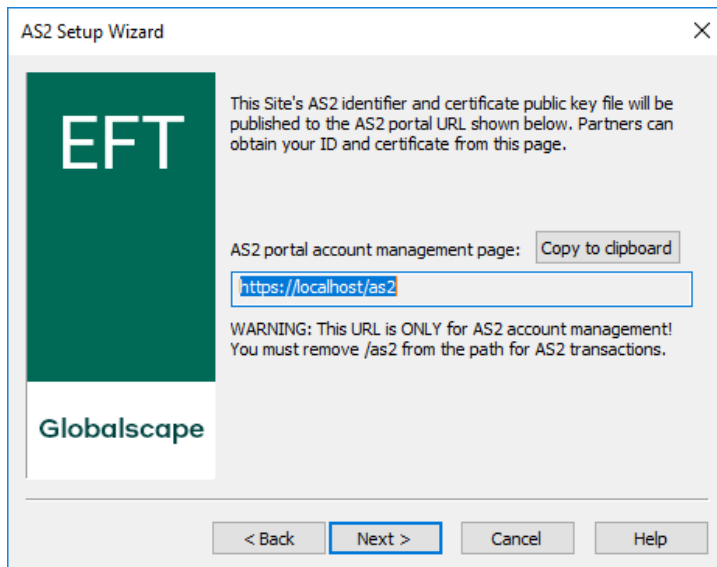
6. In the **Your AS2 Identifier** box, type the name by which you are to be identified to trading partners. (The AS2 ID cannot contain Unicode characters.)
7. Click **Next**. The **Certificate** page appears.



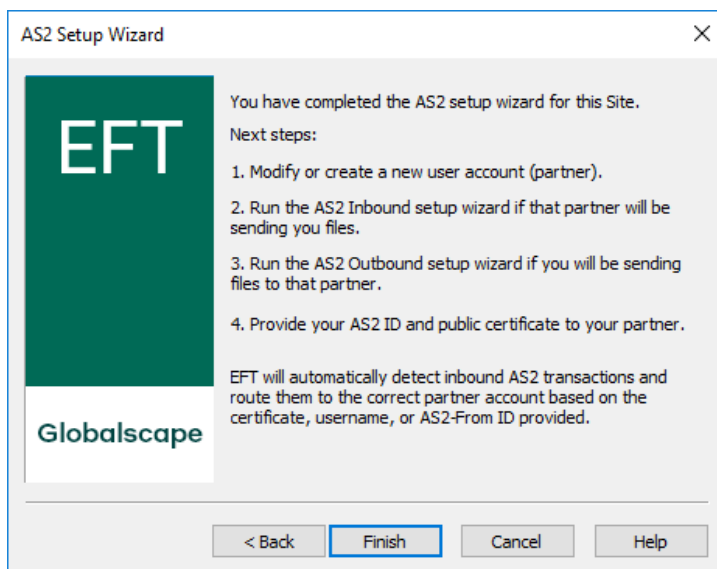
8. Do one of the following:

- 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.

Allowing AS2 Connections to a Site

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.

Allowing AS2 Connections in the Settings Template or User Account

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 630](#) 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.

AS2 Certificates

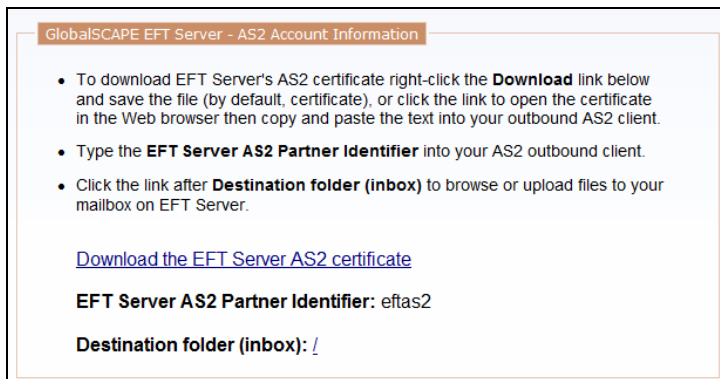
You can create certificate files using the [Certificate wizard](#). If you have a combined certificate from a third party, use the procedure in Exporting a Certificate from PFX to PEM to extract the public key.

See also: [SSL Certificate Compatibility](#).

AS2 Account Information Web Page

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 652](#), configured on the **General** tab of the partner/user account.)



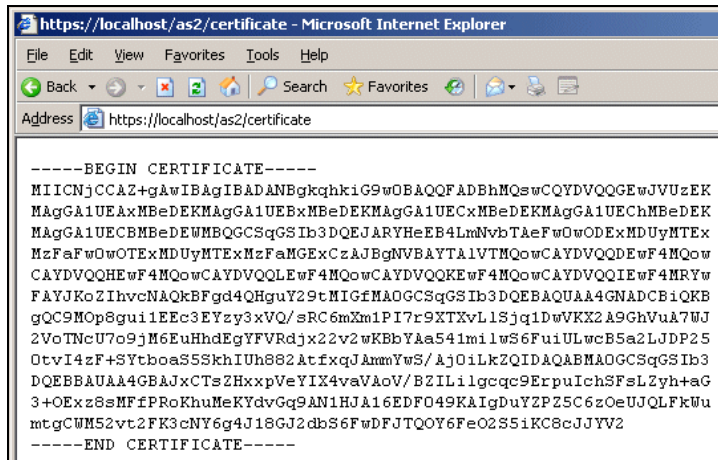
Your trading partners can access EFT's AS2 certificate from the AS2 Account Information page. Provide your trading partners with the URL of the page (for example, <https://mycompanyAS2website/as2>), then instruct them as described below. (Instructions are also provided on the Web page.)

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.)

Configuring AS2 Partners

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.

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.

Configuring AS2 Outbound Partners Using the Wizard

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.

AS2 Outbound Settings

AS2 partner profile for **outbound** (send) transactions:

Monitored hot folder:

File include mask:

File exclude mask:

Delete source files after successful offload (MDN received): ☐

Host address (prefix with 'http://' or 'https://'):

Port: 80

Path (inbox, outbox, or mailbox): /

Username:

Password:

Message subject:

Content type: Binary

Compress message: ☐

Encrypt message: ☒

Encryption algorithm: AESCBC256

Sign message: ☒

Signature algorithm: SHA-256

Your certificate: C:\ProgramData\Globalscape\...

Partner certificate:

Your AS2 identifier: adfafaf

Partner AS2 identifier:

Receipt policy: Request a signed receipt

Receipt delivery: Synchronous

Message send attempt timeout (seconds): 60

Message send attempt retries: 3

Send attempt delay between retries (seconds): 30

Asynchronous receipt timeout (minutes): 7200

Transaction FAILED notification e-mail: [\[Add\]](#)

Transaction SUCCESS notification e-mail: [\[Add\]](#)

Transaction FAILED run command: [\[Add\]](#)

Transaction SUCCESS run command: [\[Add\]](#)

Buttons: Setup Wizard, Test..., Headers..., Proxy..., Headers..., Proxy..., Clear All, OK, Cancel

- 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.

AS2 Outbound Connection Wizard

AS2 Partner Outbound Wizard

The AS2 Outbound Connection Wizard will guide you through the process of setting up the outbound profile for this partner. In an Outbound orientation, EFT is the originator and your partner is the receiver, as illustrated below.

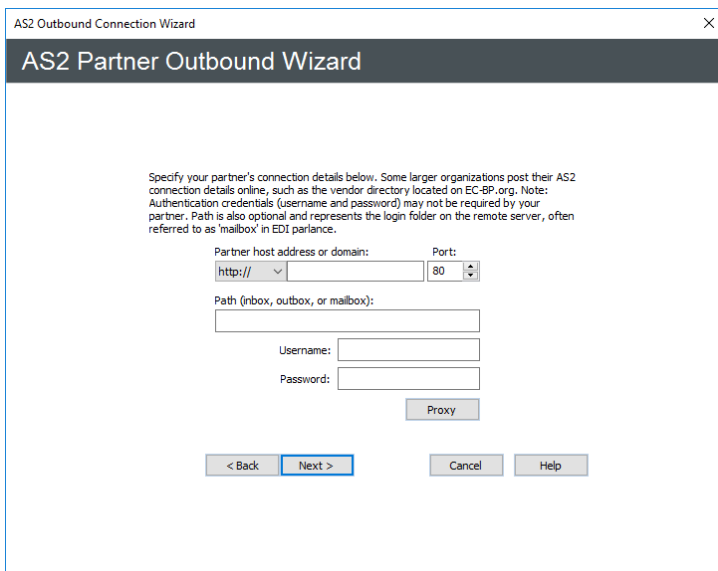
To complete the setup, the following information is required:

- + Your partner's host address.
- + Login username and password (optional).
- + Your partner's AS2 identifier.
- + Your partner's SSL certificate (public key).

If you already have this information, click "Next" to get started.

Buttons: < Back, Next >, Cancel, Help

4. Click **Next**. The AS2 partner connection information page appears.



AS2 Outbound Connection Wizard

AS2 Partner Outbound Wizard

Specify your partner's connection details below. Some larger organizations post their AS2 connection details online, such as the vendor directory located on EC-SP.org. Note: Authentication credentials (username and password) may not be required by your partner. Path is also optional and represents the login folder on the remote server, often referred to as 'mailbox' in EDI parlance.

Partner host address or domain: Port:

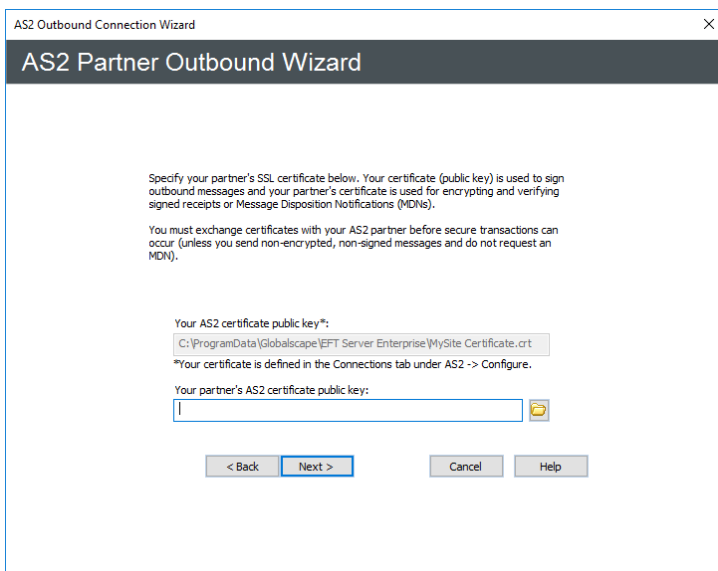
Path (inbox, outbox, or mailbox):

Username:

Password:

< Back **Next >**

- 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.
 - In the **Path** area, provide the path to the inbox, outbox, or mailbox at the AS2 partner location.
 - In the **Username** and **Password** boxes, provide the logon credentials.
 - 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.



AS2 Outbound Connection Wizard

AS2 Partner Outbound Wizard

Specify your partner's SSL certificate below. Your certificate (public key) is used to sign outbound messages and your partner's certificate is used for encrypting and verifying signed receipts or Message Disposition Notifications (MDNs).

You must exchange certificates with your AS2 partner before secure transactions can occur (unless you send non-encrypted, non-signed messages and do not request an MDN).

Your AS2 certificate public key*:

*Your certificate is defined in the Connections tab under AS2 -> Configure.

Your partner's AS2 certificate public key:

< Back **Next >**

- 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.

AS2 Outbound Connection Wizard

AS2 Partner Outbound Wizard

Choose whether to encrypt or compress the payload, and whether a receipt is required. If a receipt is necessary, specify whether it should be returned in the same session or later in a separate session once your AS2 partner has completed any post processing.

Message options

☒ Encrypt message

☒ Sign message

☐ Compress message

Receipt options

Receipt type: Request a signed receipt

Receipt return method:

☒ Return in the same session (synchronous)

☐ Return independently (asynchronous)

< Back Next > Cancel Help

- 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.

AS2 Outbound Connection Wizard

AS2 Partner Outbound Wizard

EFT can attempt to resend failed messages caused by temporary connection problems, such as a network outage. Optionally specify those retry and timeout values below.

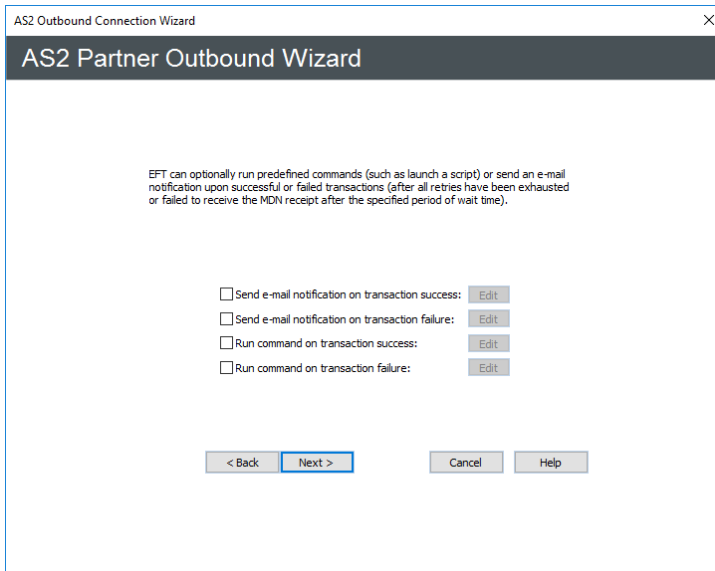
Message send attempt timeout (seconds): 60

Message retry attempts: 3

Delay between retries (seconds): 30

< Back Next > Cancel Help

- (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.)



AS2 Outbound Connection Wizard

AS2 Partner Outbound Wizard

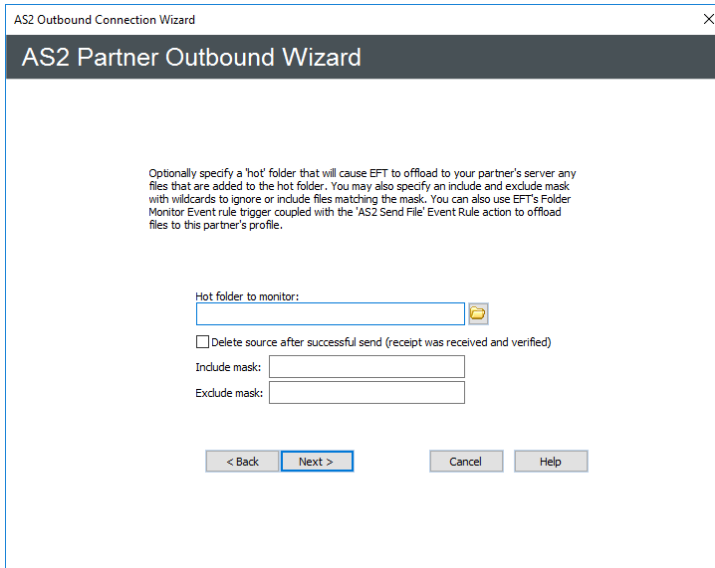
EFT can optionally run predefined commands (such as launch a script) or send an e-mail notification upon successful or failed transactions (after all retries have been exhausted or failed to receive the MDN receipt after the specified period of wait time).

☐ Send e-mail notification on transaction success: Edit
☐ Send e-mail notification on transaction failure: Edit
☐ Run command on transaction success: Edit
☐ Run command on transaction failure: Edit

< Back Next > Cancel Help

- (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.)



AS2 Outbound Connection Wizard

AS2 Partner Outbound Wizard

Optionally specify a 'hot' folder that will cause EFT to offload to your partner's server any files that are added to the hot folder. You may also specify an include and exclude mask with wildcards to ignore or include files matching the mask. You can also use EFT's Folder Monitor Event rule trigger coupled with the 'AS2 Send File' Event Rule action to offload files to this partner's profile.

Hot folder to monitor: 

☐ Delete source after successful send (receipt was received and verified)

Include mask:

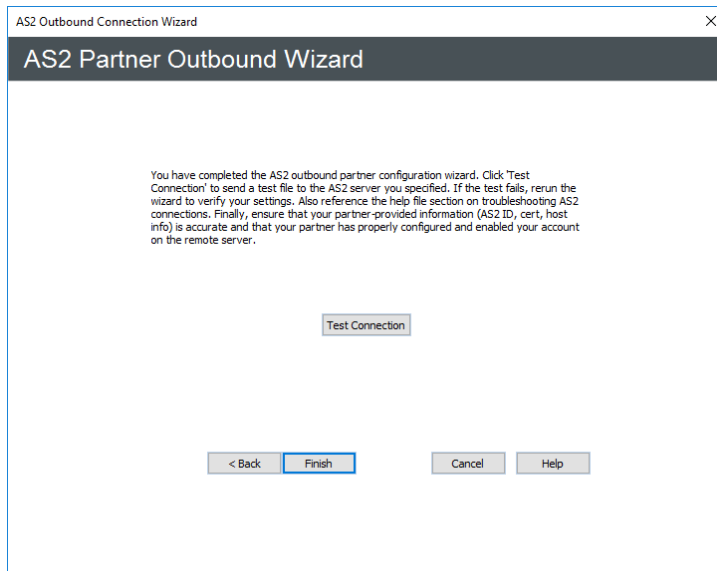
Exclude mask:

< Back Next > Cancel Help

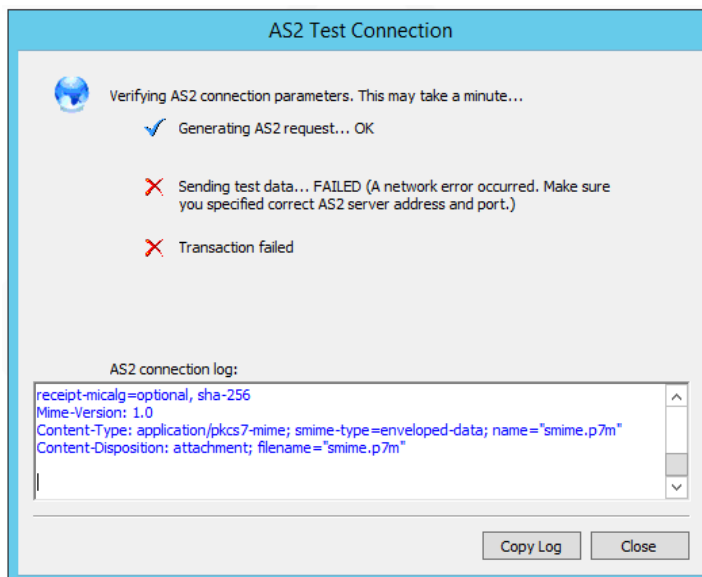
11. Specifying a folder to monitor is optional. If you specify a folder to monitor, EFT will automatically offload to your partner's AS2 server any files that are added to the specified folder. You can offload all files in the folder or only specific files or types of files. Wildcard masks can be used in the **Include mask** and **Exclude mask** boxes.

- 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

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.

General Connections Security

Specify the settings for this user.

Protocols

☐ FTP FTP configuration options: [FTP Config](#)

☐ FTPS (SSL/TLS) SSL authentication options: [SSL Auth](#)

☐ SFTP (SSH2) SFTP authentication options: [SFTP Auth](#)

☐ HTTP

☒ **HTTPS**

☒ Allow Web Transfer Client (WTC) over HTTP/S

☐ Allow Creation of Workspaces*

☐ Allow secure file sending (web and Outlook add-in)*

☒ **AS2 inbound*** [AS2 Inbound](#)

☒ **AS2 outbound*** [AS2 Outbound](#)

Network Usage & Limits

Connection limits: [Configure](#)

Transfer limits: [Configure](#)

IP access/ban list: [Configure](#)

[* Requires optional module - licensed separately](#)

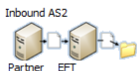
If the AS2 features are not available for the user, then AS2 is disabled on the Settings Template or the Site. [Enable and configure AS2 on the Site](#) before enabling AS2 on the Settings Template and user accounts.

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.

AS2 Inbound Connection Wizard

AS2 Partner Inbound Wizard

The AS2 Inbound Connection Wizard will guide you through the process of setting up the inbound profile for this AS2 partner. In an Inbound orientation, transactions originate with the partner and EFT is the receiver, as illustrated below.



To complete the wizard, you need to request the following information from your partner:

- + Your partner's AS2 identifier.
- + Your partner's SSL certificate (public key)

After you gather this information, click "Next" to get started.

< Back **Next >** Cancel Help

6. Click **Next**. The AS2 certificates page appears.

AS2 Inbound Connection Wizard

AS2 Partner Inbound Wizard

Specify your partner's SSL certificate (public key) below. Your certificate is required for decrypting inbound messages and for signing receipts, and your partner's certificate is required for verifying the receipt signature. You must also provide your certificate file (public key) to your partner and obtain your partner's public key in order to successfully transact with each other (unless your partner will be sending you non-encrypted, non-signed messages and does not request an MDN).

Your AS2 certificate public key*:

*Your certificate is defined in the Connections tab under AS2 -> Configure.

Your partner's AS2 certificate public key:
 

< Back **Next >** Cancel Help

- In the **Your AS2 certificate public key** box, the certificate that you specified when you created the Site appears.
- 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.

AS2 Inbound Connection Wizard

AS2 Partner Inbound Wizard

Specify your AS2 identifier (or reuse your globally defined ID) and your partner's AS2 identifier. In inbound orientation this is equivalent to your partner's "AS2-From" identifier and your "AS2-To" identifier. Sometimes (but not always) this is the Data Universal Numbering System (DUNS) number, or it can be an agreed upon identification string. Your partner can provide you with their AS2 identifier.

Your AS2 id (AS2-To):

Your partner's AS2 id (AS2-From):

Note: The AS2-From and AS2-To form a pair for identifying the Sending and Receiving Partnership. I.e. they form a composite key for identifying the parties involved in the data exchange.

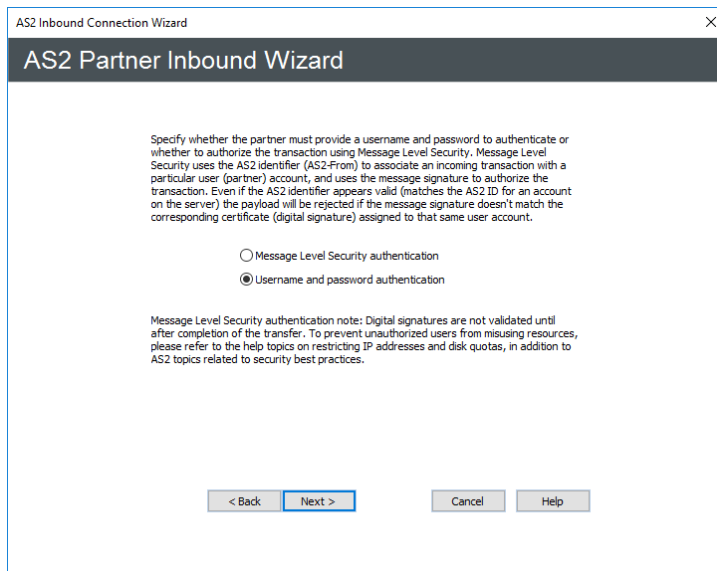
< Back **Next >** Cancel Help

- 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.



AS2 Inbound Connection Wizard

AS2 Partner Inbound Wizard

Specify whether the partner must provide a username and password to authenticate or whether to authorize the transaction using Message Level Security. Message Level Security uses the AS2 identifier (AS2-From) to associate an incoming transaction with a particular user (partner) account, and uses the message signature to authorize the transaction. Even if the AS2 identifier appears valid (matches the AS2 ID for an account on the server) the payload will be rejected if the message signature doesn't match the corresponding certificate (digital signature) assigned to that same user account.

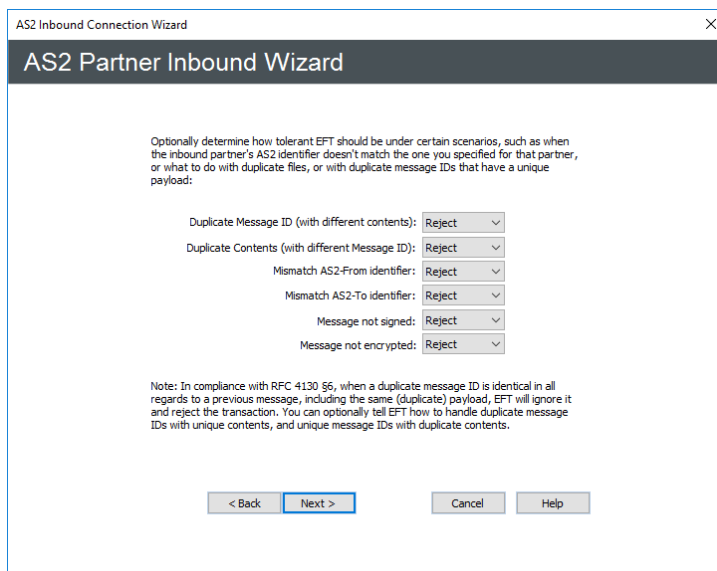
☐ Message Level Security authentication
☒ Username and password authentication

Message Level Security authentication note: Digital signatures are not validated until after completion of the transfer. To prevent unauthorized users from misusing resources, please refer to the help topics on restricting IP addresses and disk quotas, in addition to AS2 topics related to security best practices.

< Back **Next >** Cancel Help

- 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.



AS2 Inbound Connection Wizard

AS2 Partner Inbound Wizard

Optionally determine how tolerant EFT should be under certain scenarios, such as when the inbound partner's AS2 identifier doesn't match the one you specified for that partner, or what to do with duplicate files, or with duplicate message IDs that have a unique payload:

Duplicate Message ID (with different contents): Reject
 Duplicate Contents (with different Message ID): Reject
 Mismatch AS2-From identifier: Reject
 Mismatch AS2-To identifier: Reject
 Message not signed: Reject
 Message not encrypted: Reject

Note: In compliance with RFC 4130 §6, when a duplicate message ID is identical in all regards to a previous message, including the same (duplicate) payload, EFT will ignore it and reject the transaction. You can optionally tell EFT how to handle duplicate message IDs with unique contents, and unique message IDs with duplicate contents.

< Back **Next >** Cancel Help

- (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.

AS2 Inbound Connection Wizard

AS2 Partner Inbound Wizard

EFT can automatically send an e-mail notification or run a predefined command (such as launching a script) whenever a transaction is completed. Actions can be configured to run after a transaction succeeds or fails.

☐ Send e-mail notification on transaction success: [Edit](#)
☐ Send e-mail notification on transaction failure: [Edit](#)
☐ Run command on transaction success: [Edit](#)
☐ Run command on transaction failure: [Edit](#)

[< Back](#) [Next >](#) [Cancel](#) [Help](#)

- (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.

AS2 Inbound Connection Wizard

AS2 Partner Inbound Wizard

Optionally specify a location to move files received from this partner. This can be a local, shared, or UNC path name. You can keep the existing filename or use EFT's extensive selection of variables to rename the file. For more information about variables, search the Help file for keyword 'Variables'.

Optional post receipt settings:

Move received file(s) to folder:

Rename file(s) using mask:

%FS.FILE_NAME%

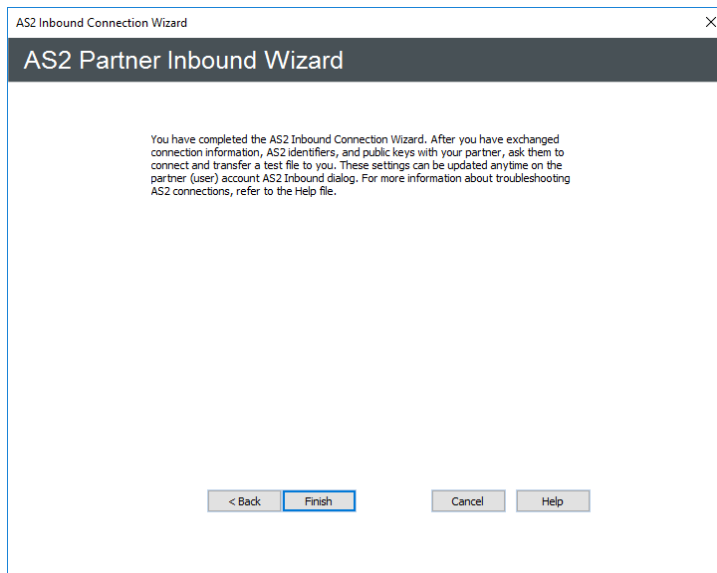
< Back Next > Cancel Help

- (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

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.)

AS2 Inbound Settings

AS2 partner profile for **inbound** (receive) transactions:

Your certificate: C:\ProgramData\Globalscap... [Setup Wizard](#)

Partner certificate: [...](#)

Your AS2 identifier: adfafaf

Partner AS2 identifier:

Authentication mechanism: Username and password

Partner AS2 identifier mismatch policy: Reject

EFT AS2 identifier mismatch policy: Reject

Duplicate Message ID with different contents: Reject

Duplicate Contents with different Message ID: Reject

Message not signed: Reject

Allowed signature algorithms: SHA1,MD5,SHA-256,SHA-38...

Message not encrypted: Reject

Allowed encryption algorithms: 3DES,AESCBC128,AESGCM1...

MDN send attempt timeout (seconds): 60

MDN send attempt retries: 3

MDN send attempt delay between retries (seconds): 30

MDN signing algorithm (MIC): As requested or SHA-256

Transaction FAILED notification e-mail: [\[Add\]](#)

Transaction SUCCESS notification e-mail: [\[Add\]](#)

Transaction FAILED run command: [\[Add\]](#)

Transaction SUCCESS run command: [\[Add\]](#)

Move received data to folder: [...](#)

Rename file(s) to:

HTTP 1.0 mode (don't send HTTP/1.1 100 Continue): ☐

[Clear All](#)

[OK](#) [Cancel](#)

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.)
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.

Parameter	Required/Optional	Description
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
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.

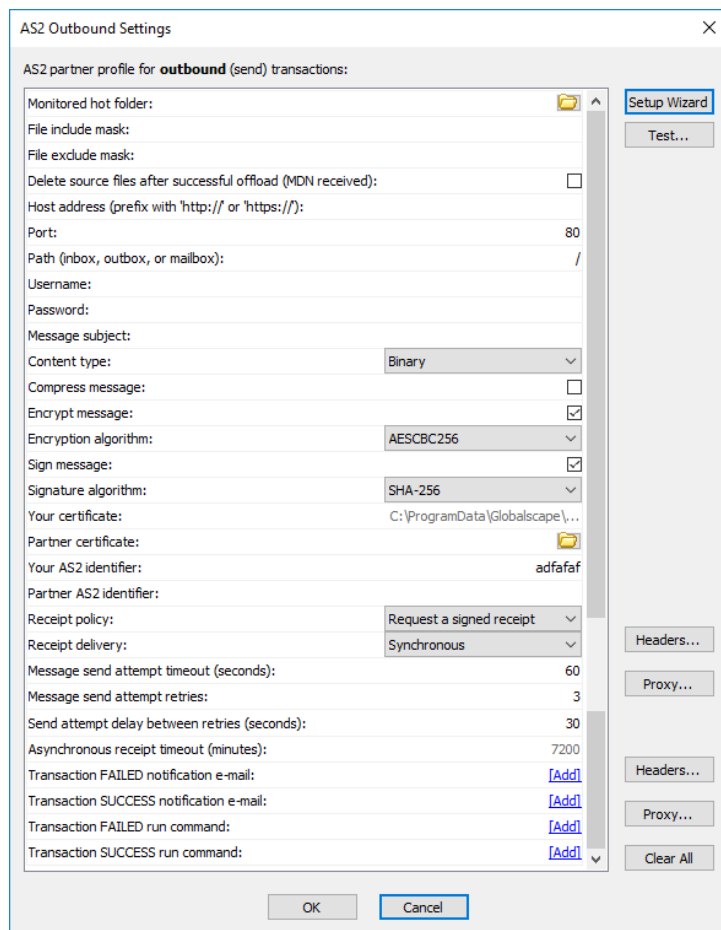
Parameter	Required/Optional	Description
Allowed encryption algorithms	Optional	Used to allow or not allow specific encryption algorithms.
MDN send attempt timeout (seconds)	Required	Specifies the timeout period after which an asynchronous MDN send attempt shall be considered a failure if no response 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.)
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.

Parameter	Required/Optional	Description
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

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 [Inheritance on page 621](#) rules apply. (AS2 has to be [enabled and configured for the Site](#) before you can enable it for a Settings Template or user account.)



AS2 Outbound Settings dialog box showing configuration for an AS2 partner profile for outbound (send) transactions.

AS2 partner profile for **outbound** (send) transactions:

Monitored hot folder: [Browse]

File include mask: [Text field]

File exclude mask: [Text field]

Delete source files after successful offload (MDN received): ☐

Host address (prefix with 'http://' or 'https://'): [Text field]

Port: 80

Path (inbox, outbox, or mailbox): /

Username: [Text field]

Password: [Text field]

Message subject: [Text field]

Content type: Binary

Compress message: ☐

Encrypt message: ☒

Encryption algorithm: AESCBC256

Sign message: ☒

Signature algorithm: SHA-256

Your certificate: C:\ProgramData\Globalscape\...

Partner certificate: [Browse]

Your AS2 identifier: adfafaf

Partner AS2 identifier: [Text field]

Receipt policy: Request a signed receipt

Receipt delivery: Synchronous

Message send attempt timeout (seconds): 60

Message send attempt retries: 3

Send attempt delay between retries (seconds): 30

Asynchronous receipt timeout (minutes): 7200

Transaction FAILED notification e-mail: [Add]

Transaction SUCCESS notification e-mail: [Add]

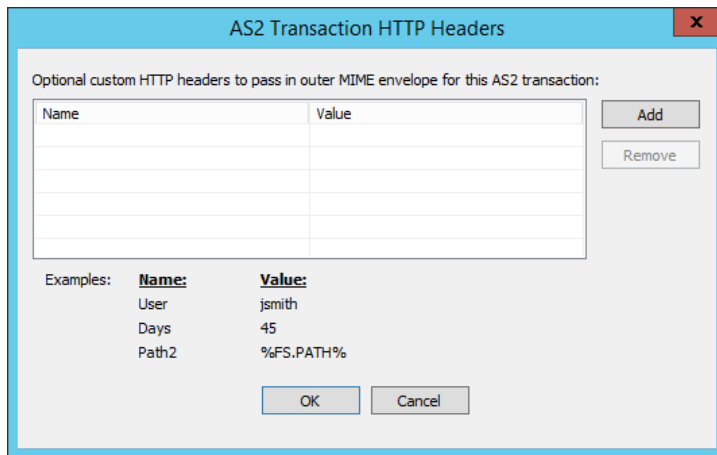
Transaction FAILED run command: [Add]

Transaction SUCCESS run command: [Add]

Buttons: Setup Wizard, Test..., Headers..., Proxy..., Clear All, OK, Cancel.

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](#)



The dialog box is titled "AS2 Transaction HTTP Headers" and has a close button (X) in the top right corner. It contains a text area for "Optional custom HTTP headers to pass in outer MIME envelope for this AS2 transaction:". Below this is a table with two columns: "Name" and "Value". To the right of the table are "Add" and "Remove" buttons. Below the table, there are "Examples:" followed by two columns: "Name:" and "Value:". The examples listed are: User (jsmith), Days (45), and Path2 (%FS.PATH%). At the bottom are "OK" and "Cancel" buttons.

Name	Value

Examples:

Name:	Value:
User	jsmith
Days	45
Path2	%FS.PATH%

- 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.
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

Parameter	Required/Optional	Description
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.)
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.

Parameter	Required/Optional	Description
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
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.)

Parameter	Required/ Optional	Description
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

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

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.

Renaming 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 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%
```

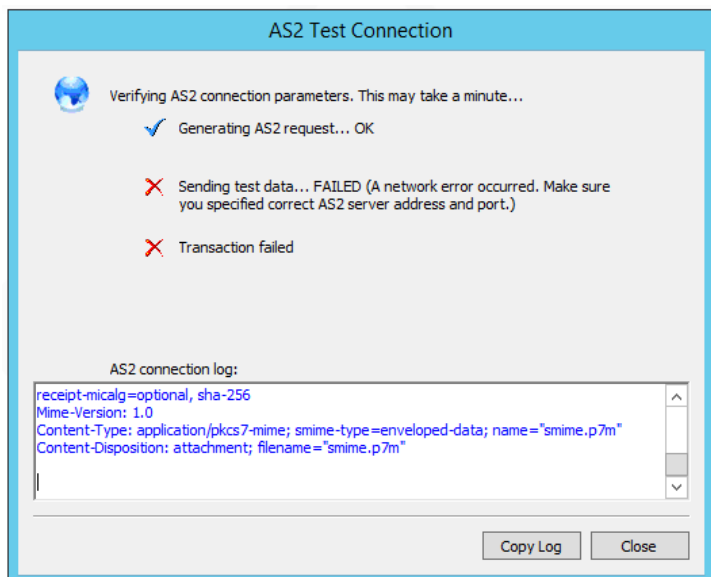
A file transferred as `dailyprogress.doc` on May 3, 2008 at 10:56:26 would be renamed to `05032008_105626_dailyprogress.doc`.

6. Click **OK** to close the AS2 Inbound Settings dialog box.
7. Click **Apply** to save the changes on EFT.

Testing the AS2 Outbound Connection

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.

Troubleshooting AS2 Issues

The AS2 module provides monitoring tools that can assist you in troubleshooting AS2 connections to EFT. See also: [Testing the AS2 Outbound Connection](#).

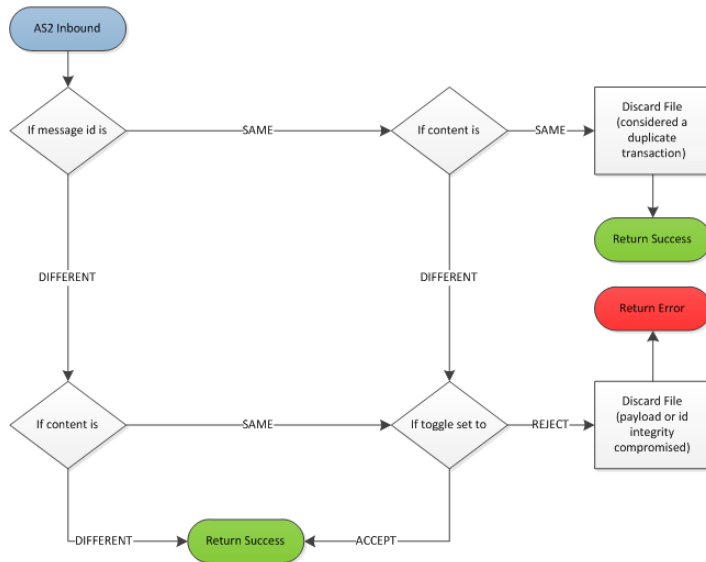
Possible reasons for AS2 file transfer failure:

- 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 address/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 Parameters](#) for 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

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 Disk Quota on page 649 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 358 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 252 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 Banner Message

When a client first connects to the Site via FTP, but before the user logs on, the *connection banner* appears. For example:

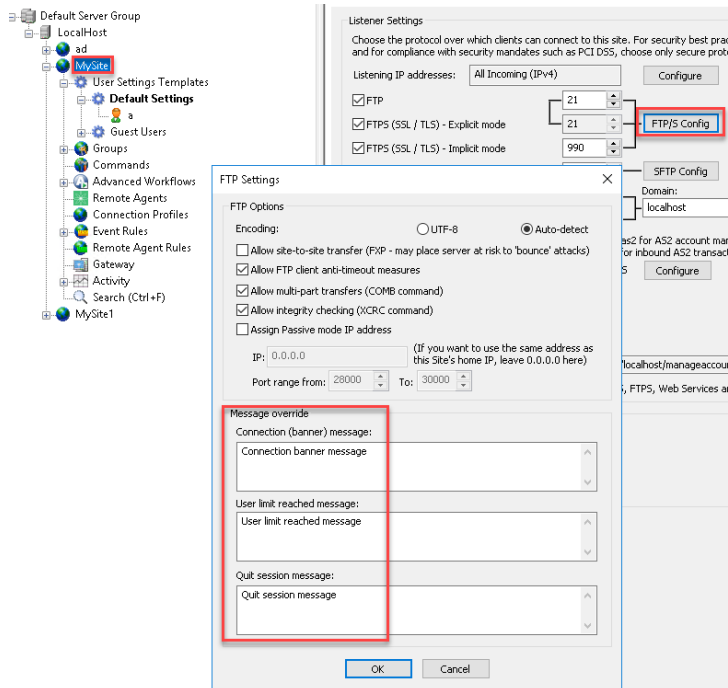
```
[8/25/2009 9:47:43 AM] 220 Globalscape EFT * UNREGISTERED COPY *
```

(UNREGISTERED COPY appears until you activate your serial number.)

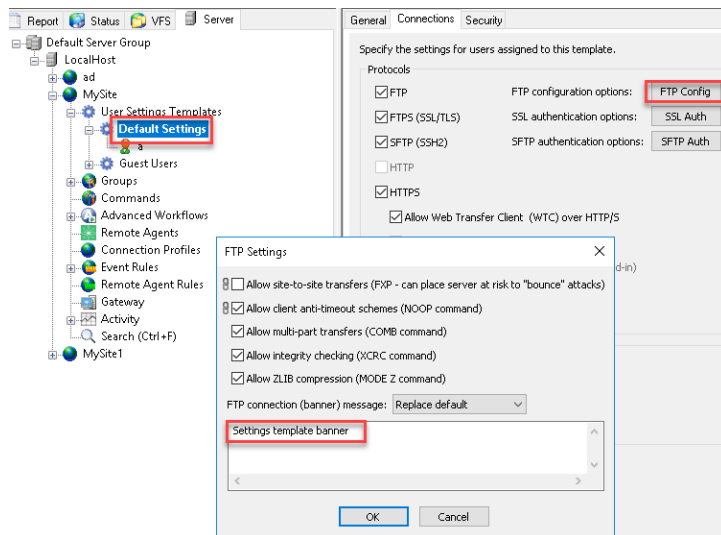
- The FTP connection banner message is configured in the **FTP Settings** dialog box on the Site.

- EFT sends two banners in **FTP or FTP/s** connections:
 - 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**.
 - 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%

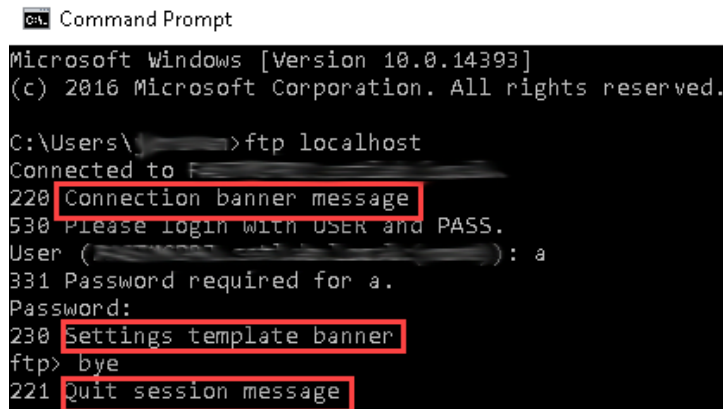
Configuring the FTP banner:



Configuring the Settings Template or SFTP banner:



FTP login sequence:



```

C:\Users\> Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\> ftp localhost
Connected to F...
220 Connection banner message
530 Please login with USER and PASS.
User (a): a
331 Password required for a.
Password:
230 Settings template banner
ftp> bye
221 Quit session message
  
```

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

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.

Content Integrity Control (CIC) uses the Internet Content Adaptation Protocol (ICAP) to connect to third party DLP and AV scanners. Create profiles on this tab and use them in the event rule CIC action to scan files for malware or potential data leaks.

Profiles

- File SCan

Request Setup

Host address: 192.168.0.1 Port: 1344

Path: /

Mode: ☒ Request modification (REQMOD) ☐ Response modification (RESPMOD)

☒ Limit scans to first: 100 KBytes

Test Connection

Headers

Response Handling

Use this section to determine how EFT should proceed when encountering connectivity, http errors, violations, or redactions.

"Fail" will trigger this action's "If Failed" routine.
 "Continue" will result in the issue being logged, but the rule will continue to the next step.

Connectivity errors: Continue

HTTP errors: Continue

ICAP violations: Fail

ICAP redactions: Continue

☒ Audit and put into variables these ICAP response "X-" headers (semicolon delimited):

<All "X-" headers>

Add Remove

To remove a profile

- To remove a profile, select its name in the list, and then click **Remove**.

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

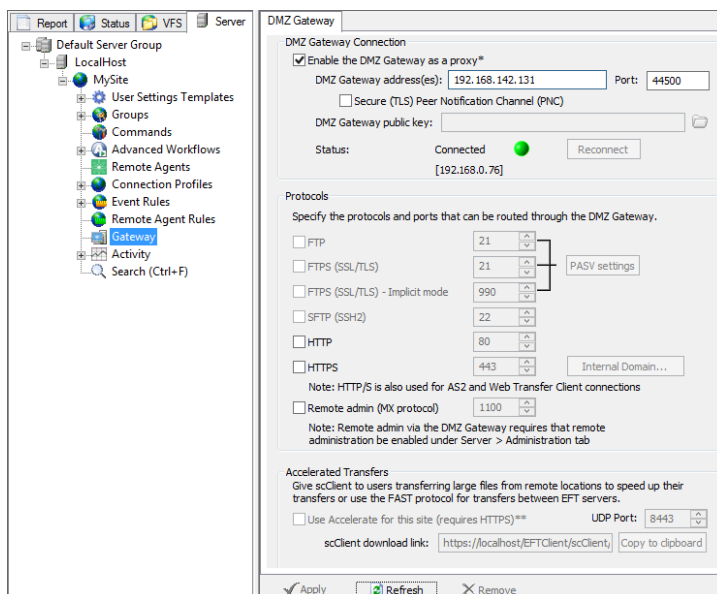
DMZ Gateway Tab - Configuring Perimeter Network Security

If you have installed the DMZ Gateway module, you must 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 with the DMZ Gateway, and 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. 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.
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.

Enabling DMZ Gateway in EFT

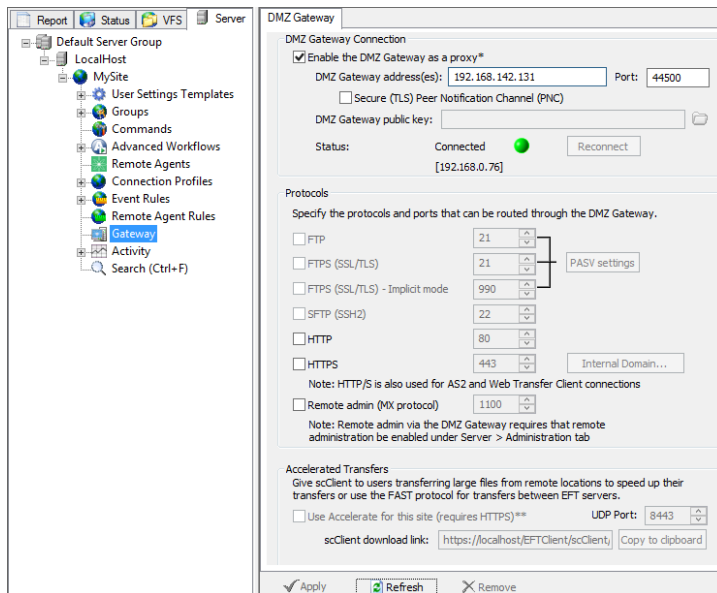
You can enable DMZ Gateway when you create the Site or enable it later in the EFT administration interface. In the Site Setup wizard, EFT displays the **Perimeter Security** configuration page that asks whether you will be using DMZ Gateway, and allows you to enter the DMZ Gateway IP address and port 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. 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.

11. 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.

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	

Ports	Purpose
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)	Inbound: Encrypted TCP connections for transferring files with EFT via FTP protocol used by FTP clients.
TCP: 989 (outbound)	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.
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

Ports	Purpose
TCP: 1521 (Oracle)	TCP Unencrypted or encrypted (SSL/TLS) connection used to save and retrieve ARM logs into SQL Server
TCP: 2484 (Oracle SSL)	
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 ICAP server 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	
UDP: 138	iSCSI ports typically used by SAN storage, and consumed by EFT as storage presented as a NTFS local drive or file shares.
DFS, Group Policy and NetBIOS used for Storage replication if used by EFT Server	
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

Ports	Purpose
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

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 102](#) 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.

Account Security

☒ Automatically create a home folder for new users

☒ Grant full permissions to users in their home folder

☐ Disable account after 90 days of inactivity*

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.

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 override](#) and [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

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)

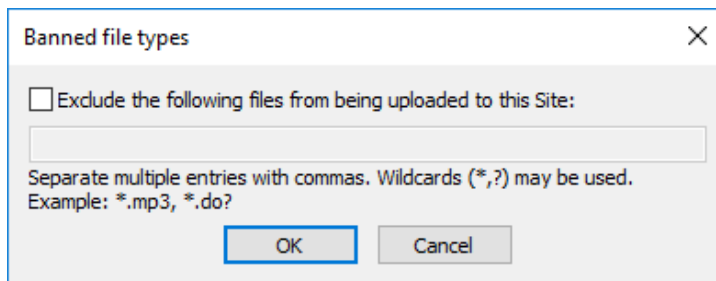
`*.wa?`

(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

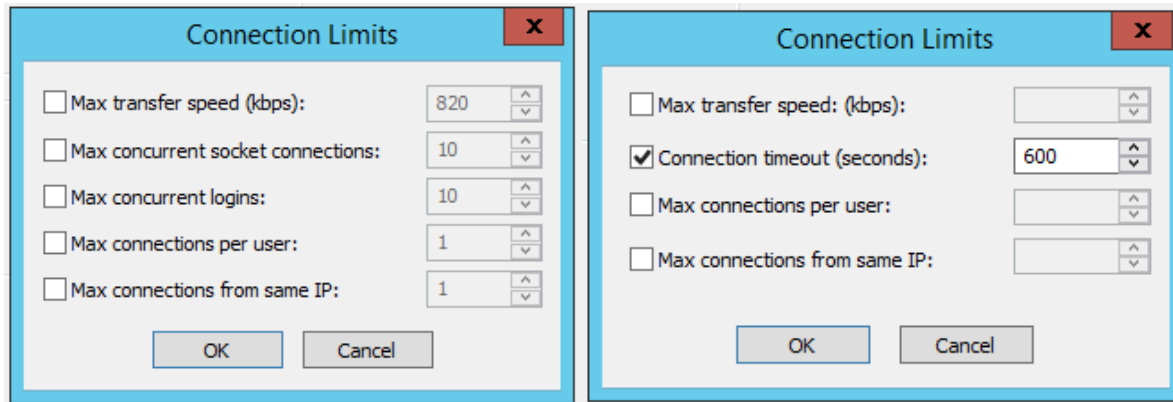
1. In the administration interface, [connect to EFT](#) and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. In the right pane, click the **Security** tab.
4. In the **Data Security** area, next to **Banned file types**, click **Configure**. The **Banned File 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.

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.

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.

The screenshot shows the 'Connections' tab in the Site Configuration interface. The 'Listener Settings' section is active, showing a list of protocols and their corresponding ports. The 'Listening IP addresses' dropdown is set to 'All Incoming (IPv4)'. The 'Configure' button is highlighted. Below the protocols, there are sections for 'AS2 Config', 'Require additional factor for HTTP/S auth:', 'Allow Globalscape Mobile Transfer Client (MTC) over HTTPS', 'Event Rule invoke over WS/SOAP (uses HTTPS port)*', 'Redirect all plaintext HTTP traffic to HTTPS*', 'Enable HSTS', and 'Enable Proxy Protocol for all protocols enabled on this Site'. The 'SSL certificate settings' and 'SSL security settings' sections are also visible. The 'Network Usage and Security Settings' section is at the bottom, with 'Connection limits', 'IP access/ban list', and 'Denial of Service settings' all having 'Configure' buttons.

4. Next to the **Listening IP addresses** box, click **Configure**. The **Listening IP Settings** dialog box appears.

The screenshot shows the 'Listening IP Settings' dialog box. It has a title bar with a close button. The 'Listening IPs:' section contains a list of IP addresses and protocols. The first item, 'All Incoming (IPv4)', is selected with a checkmark. Other items include 'All Incoming (IPv6)', 'All Incoming (IPv4 and IPv6)', '127.0.0.1', '192.168.96.131', '::1 (localhost)', '2001:0:34f1:8072:3855:2cc4:3f57:9f7c', 'fe80::3855:2cc4:3f57:9f7c%4 (link-local)', and 'fe80::3c63:7324:3026:90df%5 (link-local)'. At the bottom, there are 'OK' and 'Cancel' buttons.

- 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](#) not 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.

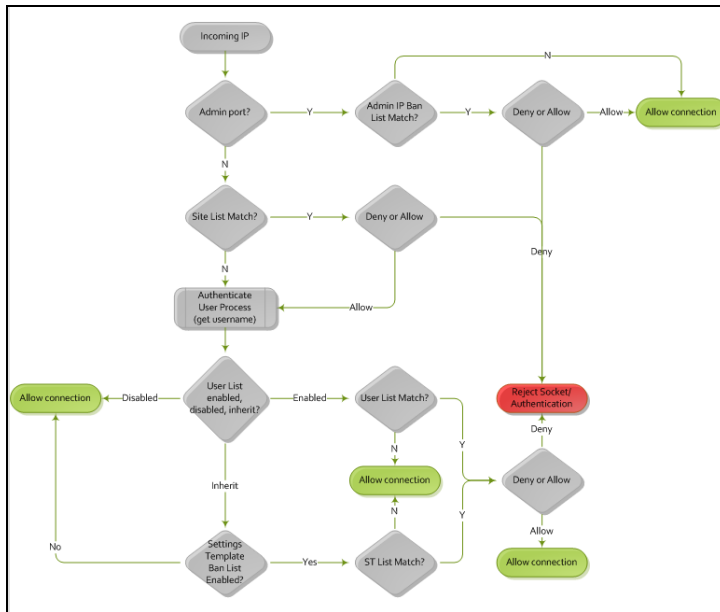
Controlling Access to the Site by IP Address

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.

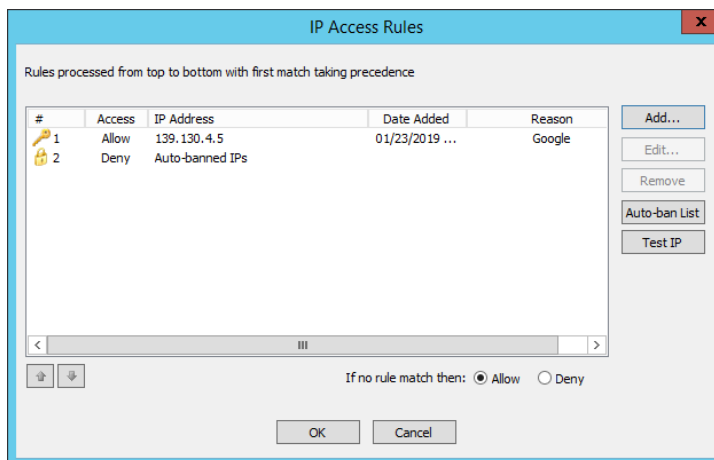
The diagram below provides a logic flow of EFT's IP address ban process.



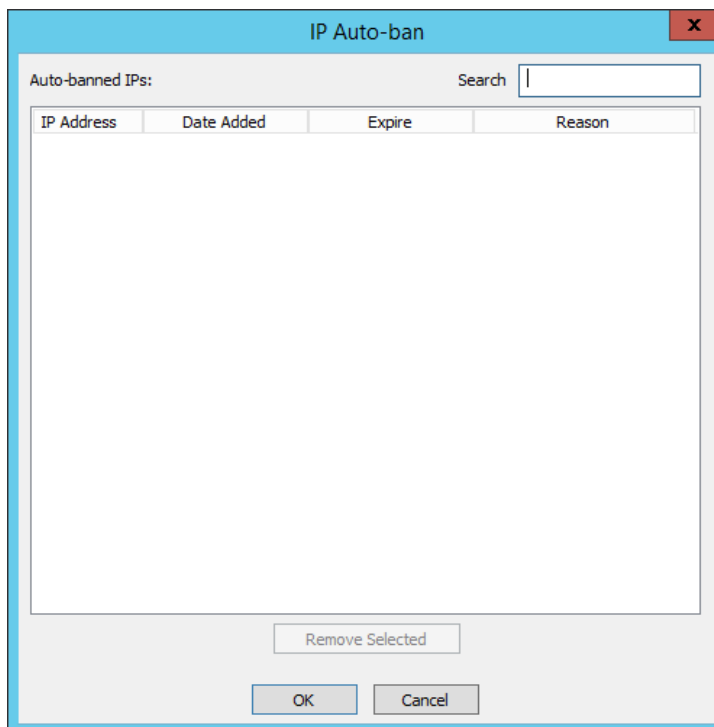
IP address policy changes are propagated to the DMZ Gateway whenever the policy is modified in the administration interface or by the auto-ban logic.

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).

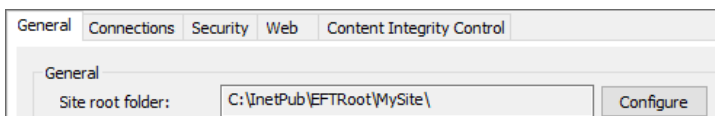
- Click **OK** to close the dialog box. The IP address/mask appears in the exceptions list.
- 4. Click **OK** to close the **IP Access Rules** dialog box.
- 5. Click **Apply** to save the changes on EFT.

Changing a Site's Root Folder

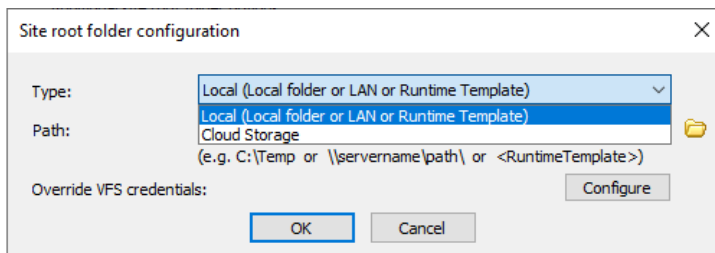
The Site root folder is specified when you [create](#) a new Site; however, you can later change a Site's root folder.

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**, then 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.

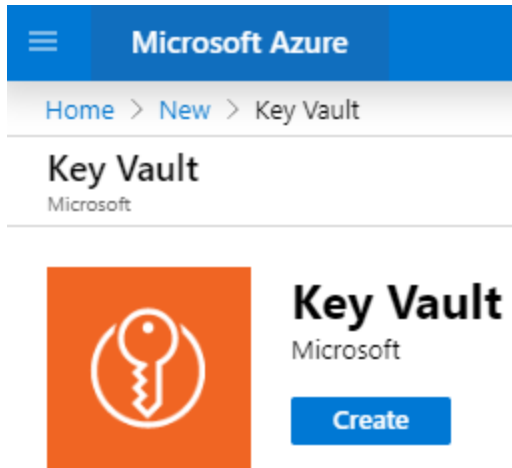
Configuring Azure Key Vault Support for EFT

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.com> and 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.

Microsoft Azure

Home > Key vaults > Create key vault

Create key vault

Basics Access policy Networking Tags Review + create

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance. [Learn more](#)

Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure subscription 1

Resource group * Select existing... [Create new](#)

Instance details

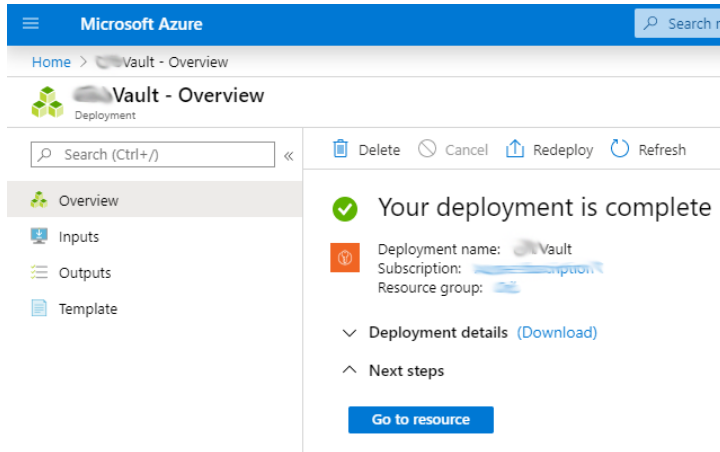
Key vault name * Enter the name

Region * North Central US

Pricing tier * Standard

[Review + create](#) < Previous Next : Access policy >

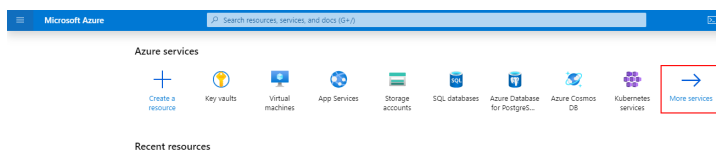
6. After providing the information above, click **Review and Create**, then click **Create**.



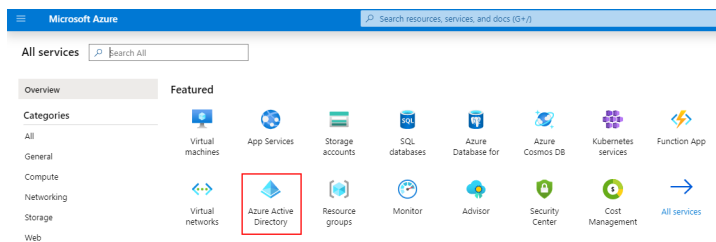
7. After **Your deployment is complete** appears, click **Go to resource**. Your Key Vault information is displayed. (Take a screen shot and save it in a secure location.)

NEXT, you will need to create an application Client ID and Client Secret

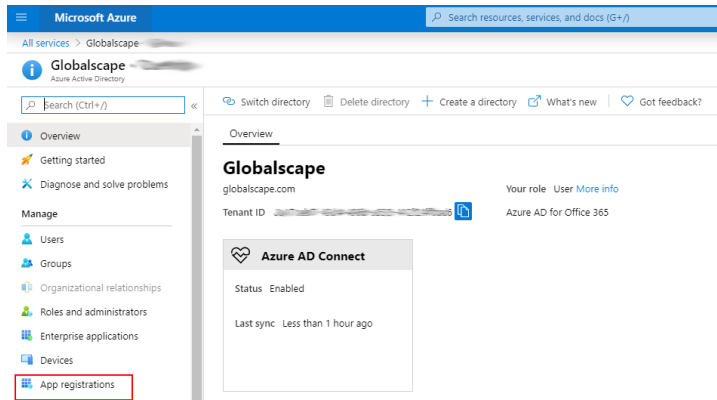
8. Under the main menu, click **Home**. The **Azure services** page appears.



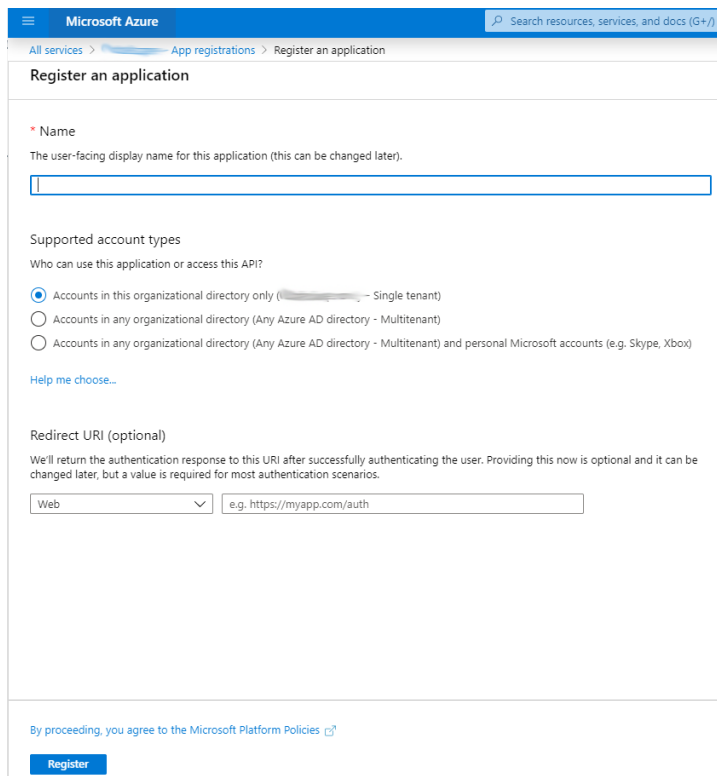
9. Click the **More services** arrow on the right.



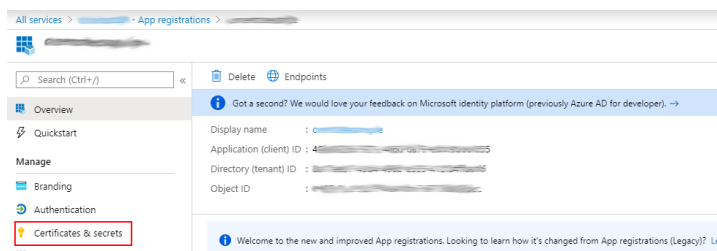
10. Click **Azure Active Directory** (Entra ID). (If your organization already has an Azure Active Directory (Entra ID) account, it will appear here, and you will need administration access to register your application (EFT).)



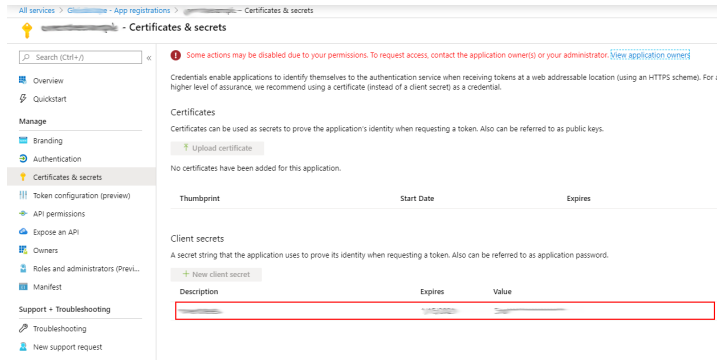
11. In the left pane, click **App registrations**.



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.)

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 [below](#) for 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

EFT Secrets	SQLite SiteConfig.<guid>.db location
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 its 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.

Secrets Module Configuration

The Secrets module allows you to choose storage for passwords, authentication tokens, passphrases, and other security artifacts used by EFT so that security and trust can be centralized.

Primary

Type: Store secrets locally, encrypting them with EFT's master secret

☒ Enable backup storage

Backup

Type: Store secrets in Azure Key Vault (AKV) via authentication token

Key Vault URL: https://mykeyvault.vault.azure.net/

Client ID:

Client Secret:

☒ Write secrets to backup in addition to primary

Tip: Uncheck if backup vault is kept in sync by third party

Test

Proxy...

OK Cancel

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 [configured](#) in 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.)

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:**

The screenshot shows a 'New Connection Profile' dialog box. At the top, there is a text field for 'Connection Profile name' containing 'New Connection Profile'. Below it is a 'Description' section with a large text area and up/down arrows. The 'Connection details' section contains several fields: 'Protocol' is a dropdown menu set to 'Cloud storage connectors'; 'Cloud provider' is a dropdown menu set to 'Azure blob storage'; 'Container URL' is a text field containing 'https://myaccount.blob.core.windows.net/mycontainer'; 'Authentication' has three radio buttons: 'Shared Key' (selected), 'Anonymous', and 'SAS'; and 'Shared key' is an empty text field. At the bottom right, there are three buttons: 'Proxy...', 'Advanced...', and 'Test'.

- Specify the **Container URL**, **Authentication** option, and **Shared key** or **SAS token**, and, if needed, [Proxy](#) and [Advanced options](#).

- **For Amazon S3:**

The screenshot shows a 'New Connection Profile' dialog box. At the top, there is a text field for 'Connection Profile name' containing 'New Connection Profile'. Below it is a 'Description' section with a large text area and up/down arrows. The 'Connection details' section contains several fields: 'Protocol' is a dropdown menu set to 'Cloud storage connectors'; 'Cloud provider' is a dropdown menu set to 'Amazon S3'; 'Bucket name' is a text field; 'S3 region' is a dropdown menu set to 'US East (Virginia) [s3.amazonaws.com]'; 'Authentication' has three radio buttons: 'Standard' (selected), 'Anonymous', and 'Requestor pays' (unchecked); 'Access key' and 'Secret key' are text fields. At the bottom right of the dialog are three buttons: 'Proxy...', 'Advanced...', and 'Test'.

- Specify the **Bucket name**, **S3 region**, **Authentication options**, **Access key**, and **Secret key**, then scroll down for [Proxy](#) and [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.
 - For more 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:

```
{
  "type": "service_account",
  "project_id": "eftgdrive",
  "private_key_id": "fe9ec8e3452b449",
  "private_key": "-----BEGIN PRIVATE
  "client_email": "eftgoogledrive@ef
  "client_id": "11117888343146682166
  "auth_uri": "https://accounts.goog
  "token_uri": "https://oauth2.googl
  "auth_provider_x509_cert_url": "ht
  "client_x509_cert_url": "https://w
}
```

NOTE: Refer to <https://cloud.google.com/iam/docs/service-accounts> for details of Google Service accounts.

Connection Profile name:

Description:

Connection details:

Protocol*:

Cloud provider:

Service account credentials:

Project ID:

Private key ID:

Client email:

Folder ID:

- 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.

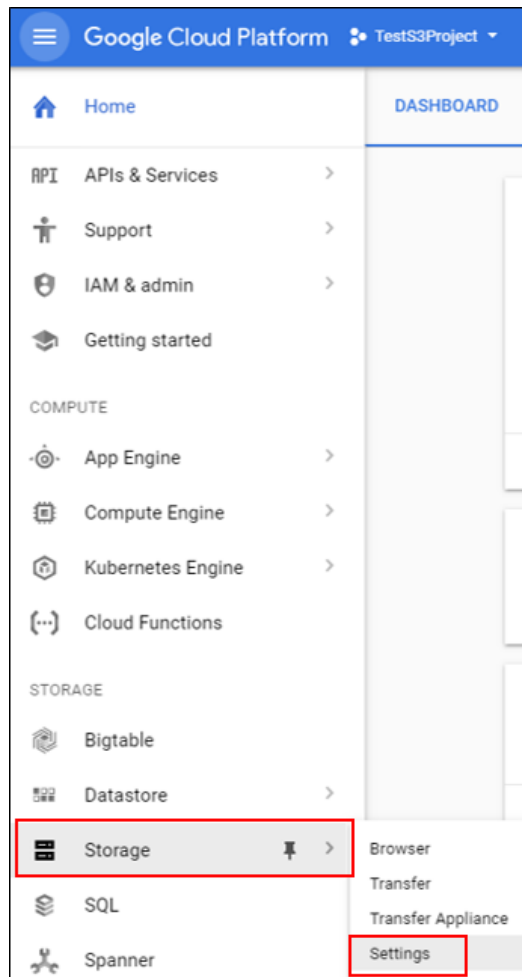
<https://drive.google.com/drive/folders/1-Si2qnf4I7FxyMDZRshPMcIO15XRpk31>

Folder ID

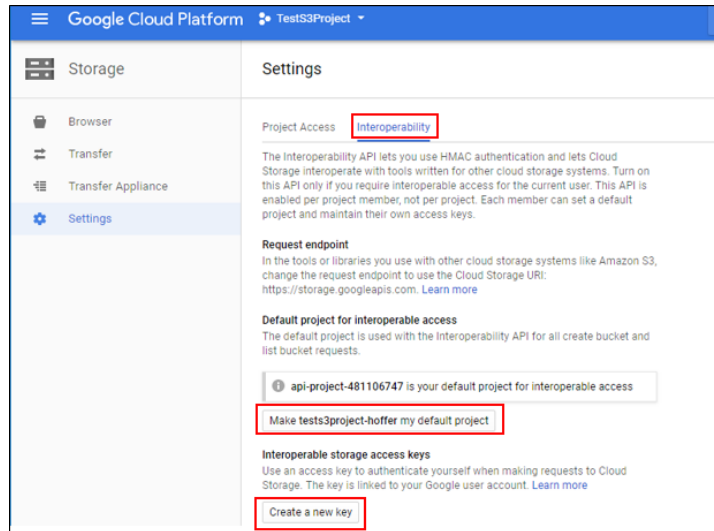
- **Alternatively, for Google Drive using Amazon S3:**

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**.

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.

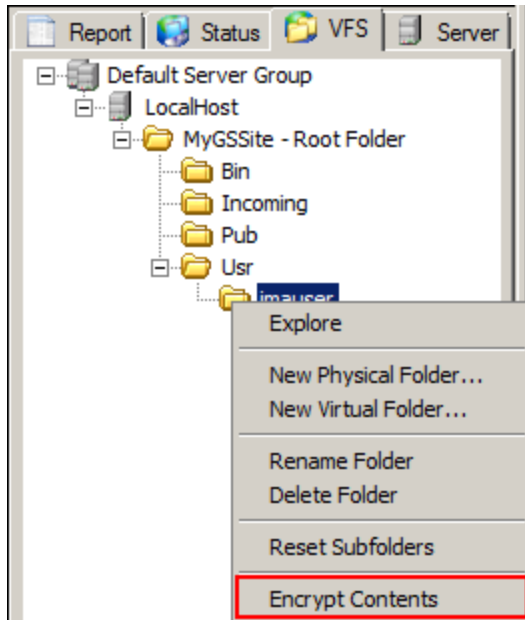
Enabling EFS Encryption

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

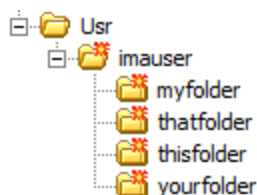
1. In the administration interface, [connect to EFT](#) and click the **VFS** tab.
2. In the left pane, right-click the parent folder you want to configure, and then click **Encrypt Contents**.



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**.

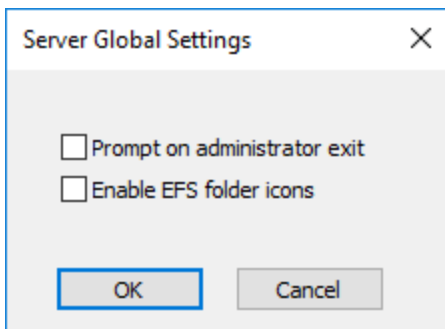
Enable EFS Folder Icons

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.)

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.

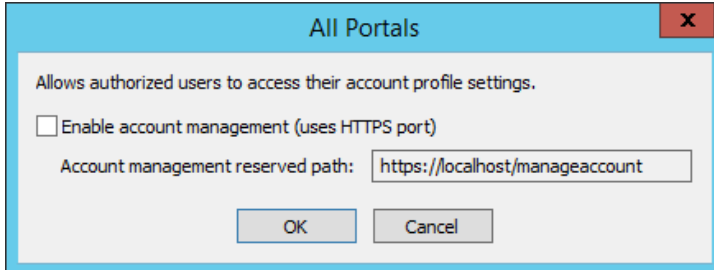
The account management page is hard-coded to `https://<server-URL>/manageaccount` with the default port of 443. If the HTTPS port is set to a different port, the user must provide the port number in the URL to log into the page (for example, `https://192.168.123.456/manageaccount:4433`).

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 [SSL](#) to 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.

Encryption in EFT

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).

- **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-channelled 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 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 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 be 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 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

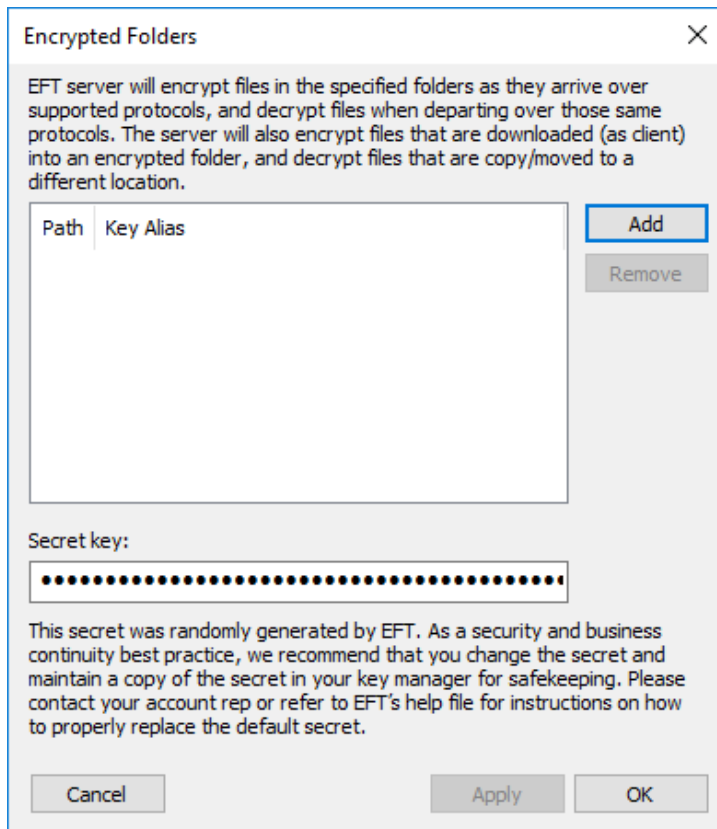
If you want to encrypt the contents of all data in the Site root, and also want to use a user-specific encryption key.

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 result 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.

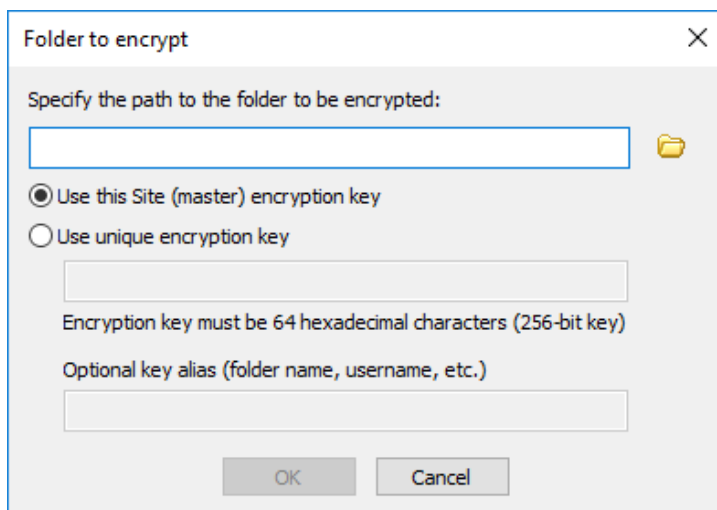
Enabling EFT-Managed Encryption

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.

Encrypted Folders

EFT server will encrypt files in the specified folders as they arrive over supported protocols, and decrypt files when departing over those same protocols. The server will also encrypt files that are downloaded (as client) into an encrypted folder, and decrypt files that are copy/moved to a different location.

Path	Key Alias

Add Remove

Secret key:

.....

This secret was randomly generated by EFT. As a security and business continuity best practice, we recommend that you change the secret and maintain a copy of the secret in your key manager for safekeeping. Please contact your account rep or refer to EFT's help file for instructions on how to properly replace the default secret.

Cancel Apply OK

- 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**.

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](#)

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.

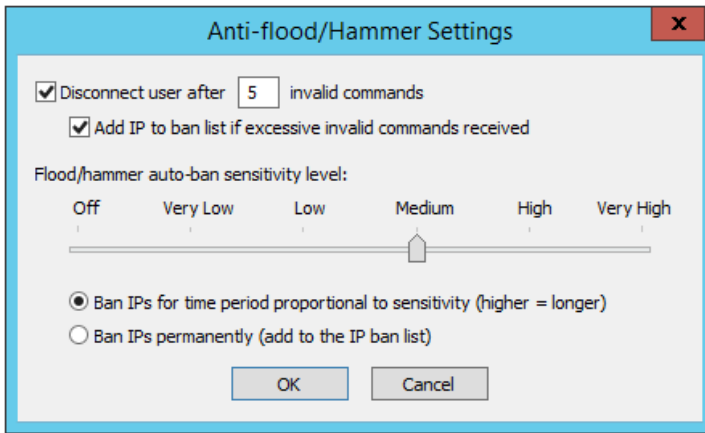
Apart from the availability protections mentioned on this page, EFT includes additional protections against confidentiality and integrity attacks. Some of those are configurable, such as failed login attempt ban logic, password complexity rules, username blacklisting, IP white/blacklisting, banned file 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)

Security Level Characteristics – HTTP(S) Session Counter	User	Very Low	Low	Medium	High	Very High
- 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

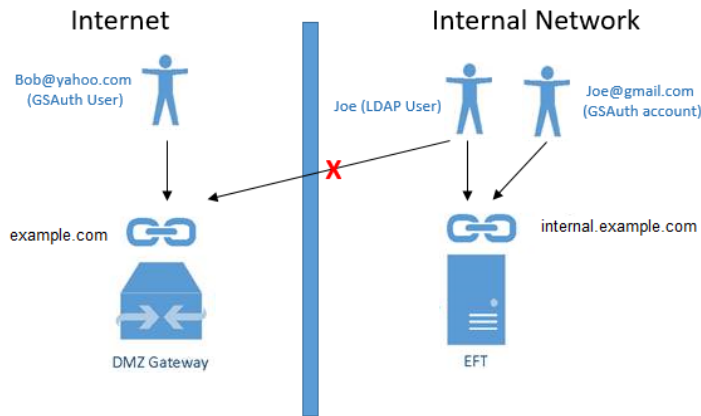
Custom Scores for Admin Session

To designate a different sensitivity level for Administrative sessions, please use the advanced property: [AutobanSensitivityLevelForAdminConnections](#)

Internal Domain Settings

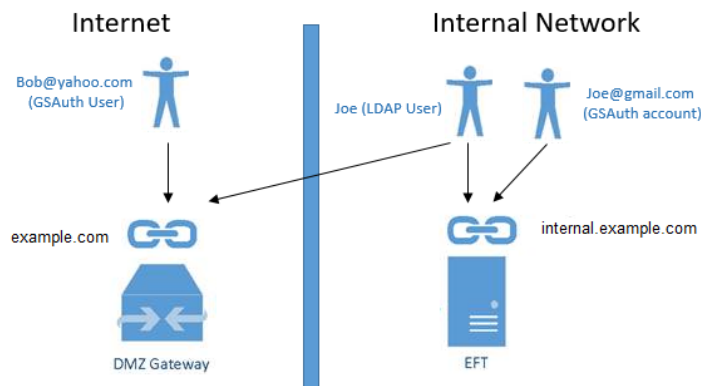
The **Internal Domain Settings** dialog box on the **DMZ Gateway** tab, is used to configure separate external and internal domain access. See [Specifying External and Internal Domains](#) and [Allow LDAP Authentication through DMZ](#) for more information about how to do that. Below are some diagrams 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.



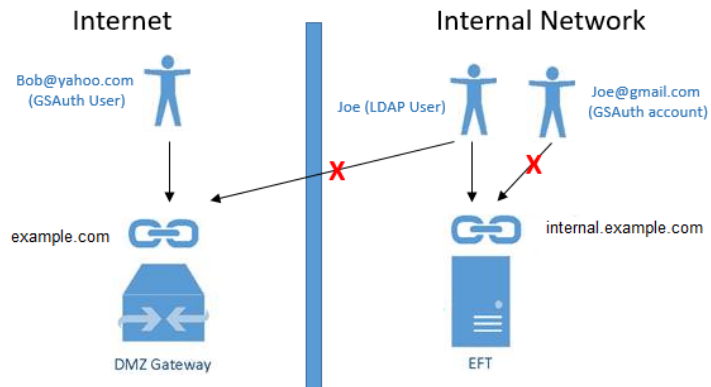
2. When the **Allow AD/LDAP authentication to EFT through DMZ Gateway** check box is selected, (but **not** the **Make AD/LDAP authentication exclusive for internal connections** check box):

- 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.



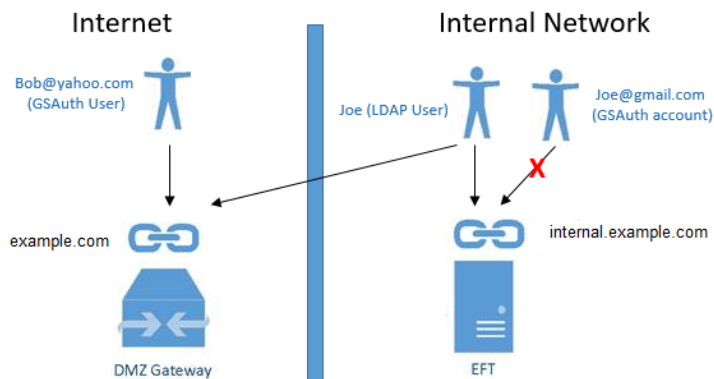
3. When the **Make AD/LDAP authentication exclusive for internal connections** check box is selected (but **not** the **Allow AD/LDAP authentication to EFT through DMZ Gateway** check box):

- 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:

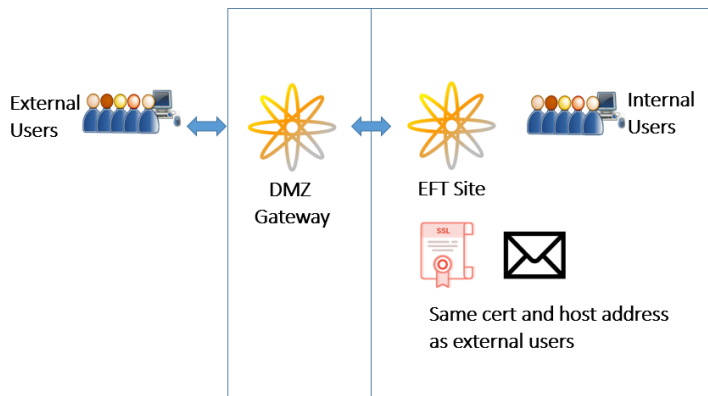
- Only AD or LDAP users can log in using the internal (EFT) or external (DMZ Gateway) URL
- Globalscape authentication users can only log in using the external (DMZ Gateway) URL; they cannot log in using the internal (EFT) URL.



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.

The screenshot shows the 'Internal Domain Settings' dialog box. It has a title bar with 'Internal Domain Settings' and a close button (X). The main content area contains the following text: 'This is an optional setting to be used if both internal and external users will be accessing EFT both through the DMZ Gateway and directly.' Below this text are three input fields: 'Internal host name:', 'SSL certificate settings:', and 'Internal email domain(s):'. The 'SSL certificate settings:' field has a 'Configure' button next to it. Below the 'Internal email domain(s):' field is a hint: 'e.g. domain.local; *internal.local'. At the bottom, there are three checkboxes: 'Allow AD/LDAP authentication to EFT through DMZ Gateway', 'Make AD/LDAP authentication exclusive for internal connections', and 'Require 2nd factor auth for internal users, if configured'. At the very bottom are 'OK' and 'Cancel' buttons.

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:

The screenshot shows the 'Connections' tab of the EFT Site Configuration interface. Under 'Listener Settings', the 'Domain' field for the HTTPS (SSL) port (443) is highlighted with a red box and contains the value '192.168.100.129'. Other protocols and ports shown include FTP (21), FTPS (21, 990), SFTP (22), HTTP (80), and AS2* (443).

An **Internal Domain** button is available next to the **HTTPS** port box on the **DMZ Gateway** tab of the EFT Site:

The screenshot shows the 'DMZ Gateway' tab of the EFT Site Configuration interface. The 'Internal Domain...' button is highlighted with a red box. An 'Internal Domain Settings' dialog box is open, showing fields for 'Internal host name', 'SSL certificate settings', and 'Internal email domain(s)'. The dialog also includes checkboxes for 'Allow AD/LDAP authentication to EFT through DMZ Gateway', 'Make AD/LDAP authentication exclusive for internal connections', and 'Require 2nd factor auth for internal users, if configured'.

To specify the internal domain on a site

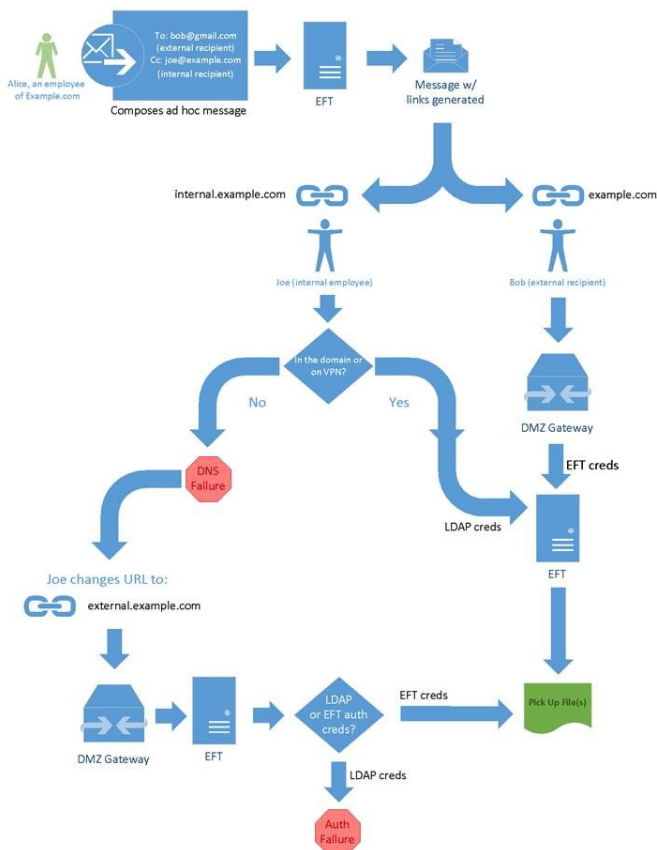
1. In the EFT administration interface, click the **Server** tab, then click the **Gateway** node.
2. On the **DMZ Gateway** tab, next to the **HTTPS** port box, click **Internal Domain**. The **Internal Domain Settings** dialog box appears.
3. In the **Internal host name** box, specify the URL through 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:

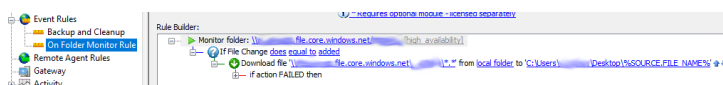
- If EFT sends an email where the email domain (after the "@" symbol) matches one of the specified "internal domains" values, any URLs formed by EFT and pointing to EFT in the email should be constructed using the internal host name (for example, internal.example.com).
- If EFT sends an email where the 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.



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.

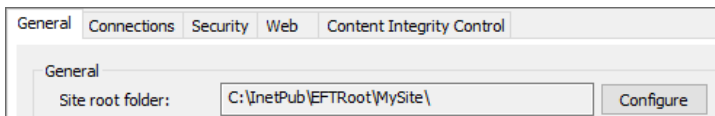
- **This topic assumes you've already created your Azure account.** Refer to <https://azure.microsoft.com/en-us/services/storage/data-lake-storage/> to read more about Azure Data Lake Storage.
- Containers created with Data Lake Gen 2 support can be monitored by an [EFT Folder Monitor Event](#) as long as the Azure container credentials and Active Directory domain trust relationship is enabled.



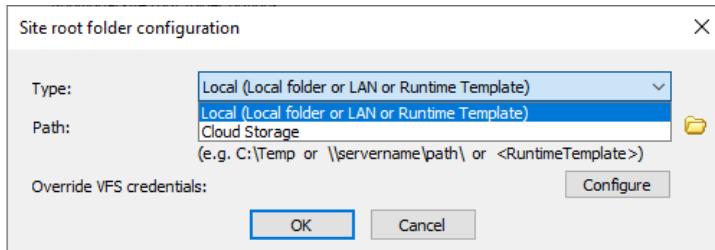
To enable the VFS credential override

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.

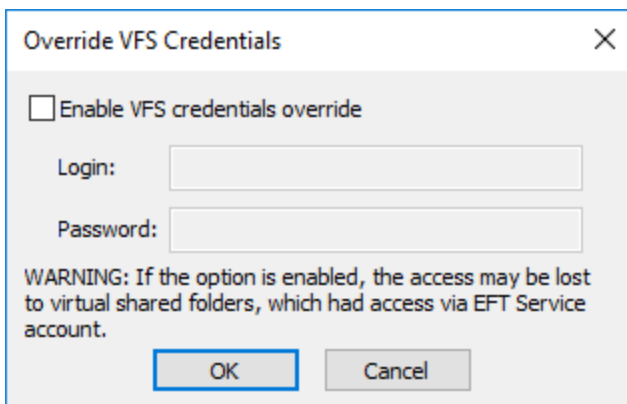
3. In the right pane, click the **General** tab.



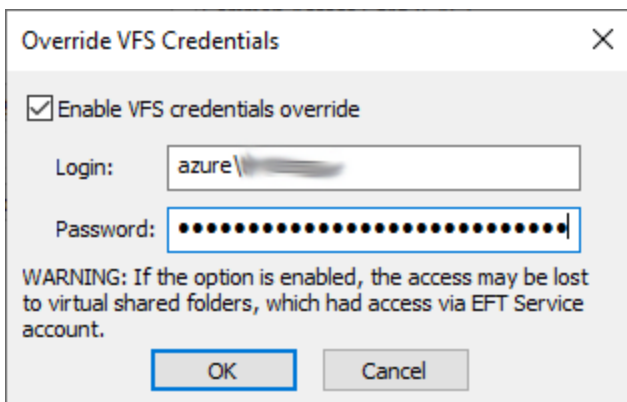
4. Next to the **Site root folder** box, click **Configure**. The **Site root folder configuration** dialog box appears.



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:

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...

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.txt> to read more.

The screenshot shows the 'Connections' tab in the EFT administration interface. The 'Listener Settings' section is expanded, displaying a list of protocols and their configurations. The 'Enable Proxy Protocol for all protocols enabled on this Site' checkbox is highlighted with a red box. Below this, there are sections for 'SSL certificate settings', 'SSL security settings', and 'Network Usage and Security Settings'.

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:

☐ FTP

☐ FTPS (SSL / TLS) - Explicit mode

☐ FTPS (SSL / TLS) - Implicit mode

☐ SFTP (SSH2)

☐ HTTP

☒ HTTPS (SSL)

☐ AS2* - Use yourdomain/as2 for AS2 account management
- Use yourdomain for inbound AS2 transactions

☐ Require additional factor for HTTP/S auth:*

☒ Allow Globalscape Mobile Transfer Client (MTC) over HTTPS

☐ 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: (Applies to HTTPS, FTPS, Web Services and AS2)

SSL security settings:

Network Usage and Security Settings

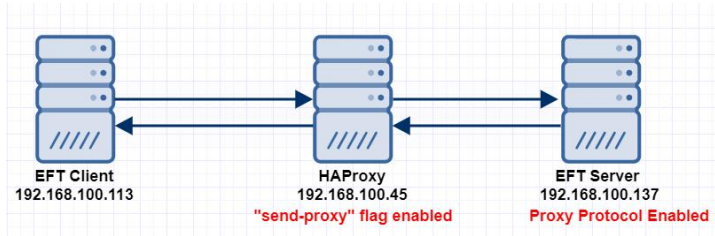
Connection limits:

IP access/ban list:

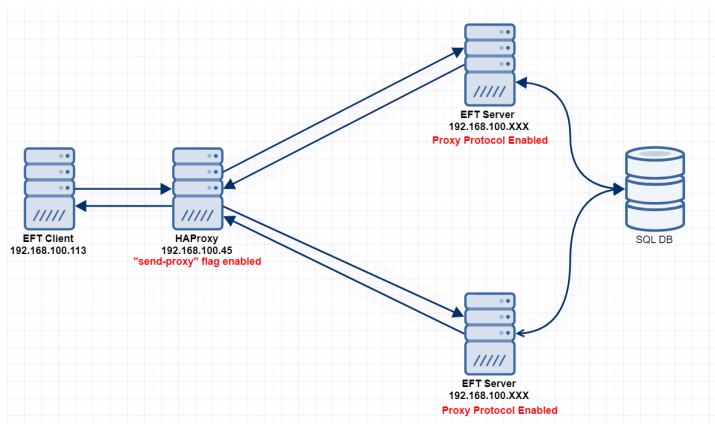
Denial of Service settings:

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.

```
#####  
# SFTP - Config #####  
#####  
frontend sftp-in  
  bind *:42  
  mode tcp  
  option tcplog  
  default_backend sftp-backend  
  
backend sftp-backend  
  #balance roundrobin  
  mode tcp  
  #server AA-2019-4 192.168.100.46:42 check  
  server AA-2019-4 192.168.100.46:42 send-proxy  
  #server AA-2019-4 192.168.100.46:42 send-proxy  
  #server AA-2019-4 192.168.100.137:42 send-proxy  
  #server AA-2019-4 192.168.100.137:42 check
```

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
```

The screenshot shows a terminal window with the following content:

```

File Edit Selection View Go Run Terminal Help

Welcome x

Start
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Customize

testuser@Ubuntu1804:~$ sudo service haproxy restart
[sudo] password for testuser:
testuser@Ubuntu1804:~$ sudo service haproxy status
● haproxy.service - HAProxy Load Balancer
   Loaded: loaded (/lib/systemd/system/haproxy.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-01-22 07:49:04 CST; 10s ago
     Docs: man:haproxy(1)
           file:///share/doc/haproxy/configuration.txt.gz
   Process: 69520 ExecStartPre=/usr/sbin/haproxy -f $CONFFIG -c -q $EXTRA_OPTS (code=exited, status=0/SUCCESS)
   Main PID: 69521 (haproxy)
      Tasks: 2 (limit: 4032)
     Group: /system.slice/haproxy.service
           └─69521 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -p /run/haproxy.pid
             └─69522 /usr/sbin/haproxy -c -f /etc/haproxy/haproxy.cfg -p /run/haproxy.pid

Jan 22 07:49:04 Ubuntu1804 haproxy[69521]: Proxy http-backend started.
Jan 22 07:49:04 Ubuntu1804 haproxy[69521]: Proxy sftp-in started.
Jan 22 07:49:04 Ubuntu1804 haproxy[69521]: Proxy sftp-in started.
Jan 22 07:49:04 Ubuntu1804 haproxy[69521]: Proxy sftp-backend started.
Jan 22 07:49:04 Ubuntu1804 haproxy[69521]: Proxy ftp-in started.
Jan 22 07:49:04 Ubuntu1804 haproxy[69521]: Proxy ftp-in started.
Jan 22 07:49:04 Ubuntu1804 haproxy[69521]: Proxy ftp-backend started.
Jan 22 07:49:04 Ubuntu1804 haproxy[69521]: Proxy ftp-backend started.

```

This is an example of what the log captures:

```
01-27-21 20:49:36,194 [2196] TRACE DMZSupport <> - DMZ: socket 302: is ready for writing. State 2
01-27-21 20:49:36,194 [2196] TRACE DMZSupport <> - DMZ: socket 302: is ready for reading. State 2
01-27-21 20:49:36,194 [2196] TRACE DMZSupport <> - DMZ: socket 302: passing to Proxy Protocol subsystem
01-27-21 20:49:36,194 [2196] WARN IPAccess <MsgSite.VerifyAddress 192.168.100.112> - Site access denied for IP: 192.168.100.112
01-27-21 20:49:36,194 [2196] WARN Common <> - Proxy Protocol: "192.168.100.112 is not allowed"
01-27-21 20:50:46,903 [7868] DEBUG DMZSupport <> - CSingleGateway::OnMessageClientEX() : verifying address: 192.168.100.45
01-27-21 20:50:46,903 [7868] DEBUG DMZSupport <> - CSingleGateway::OnMessageClientEX() : starting gateway client socket;
```

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

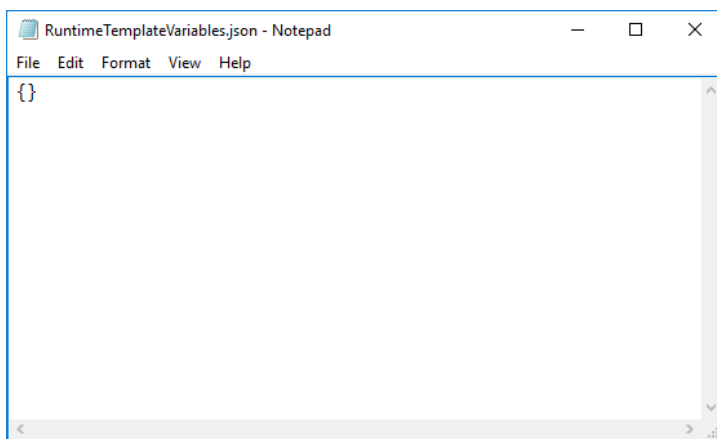
1. Log out of the administration interface.
2. Stop the EFT server service.
3. Open the SiteConfig<GUID>.db file in the SQLite DB Browser. (<https://sqlitebrowser.org/>)
4. On the **Browse Data** tab, open the Site table.
5. Edit the Site **Name**.
6. Start the EFT server service.
7. Log in to the EFT 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 reading 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:

The screenshot shows a 'File Download Configuration' dialog box. It contains the following fields and options:

- Connection Profile:** A dropdown menu set to 'None - Manually Specify'.
- Connection details:** A section containing:
 - Download method:** A dropdown menu set to 'FTP (standard File Transfer Protocol)'.
 - Host address:** A text input field containing the template '<type><host>'. This field is highlighted with a red rectangle.
 - Port:** A text input field containing the template '<port>'.
 - Username:** A text input field containing the template '<my.login>'.
 - Password:** A text input field filled with asterisks.
- Authentication:** A checkbox labeled 'Use connected client's login credentials to authenticate (refer to Site-wide Security settings to allow this option)' is unchecked.
- Buttons:** At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

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  Search (Ctrl+F) 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.

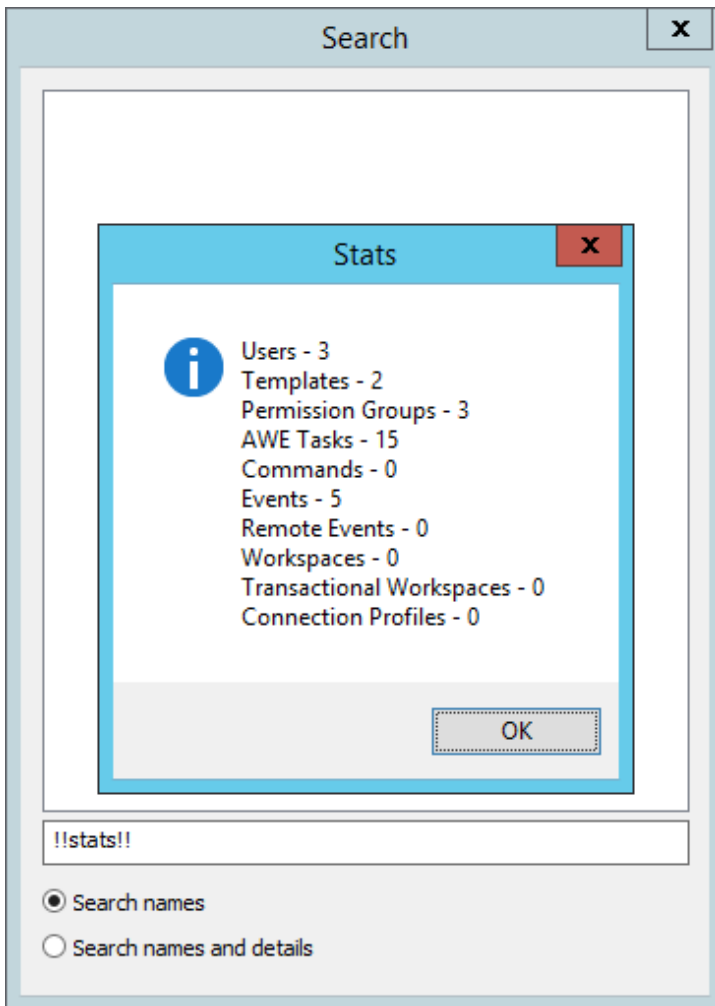
If you enter a character that is not found in any strings, the "<<NO MATCHES FOUND!>>" message appears.

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

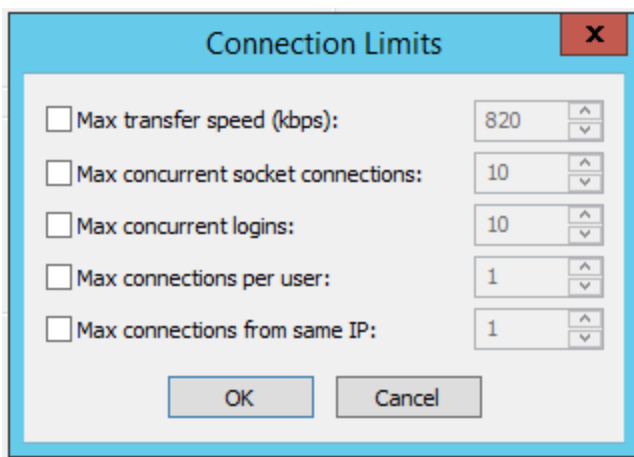
The **Max concurrent socket connections** check box limits the amount of socket or low-level connections on a Site allowed by EFT. When this limit is reached, any subsequent connection attempt generates a socket or network error in the client. It reacts as if EFT is not available, because EFT refuses 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.



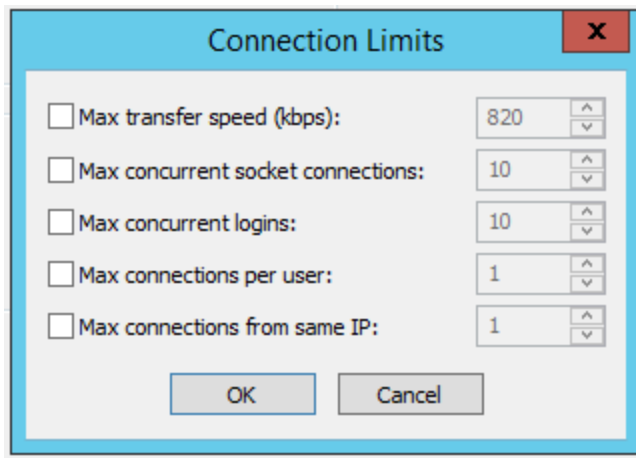
5. Select the **Max concurrent socket connections** check box, then specify the maximum number of users you want to allow at any given time. If the box is cleared, EFT does not restrict the number of users.
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

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.

Setting Maximum Connections per User

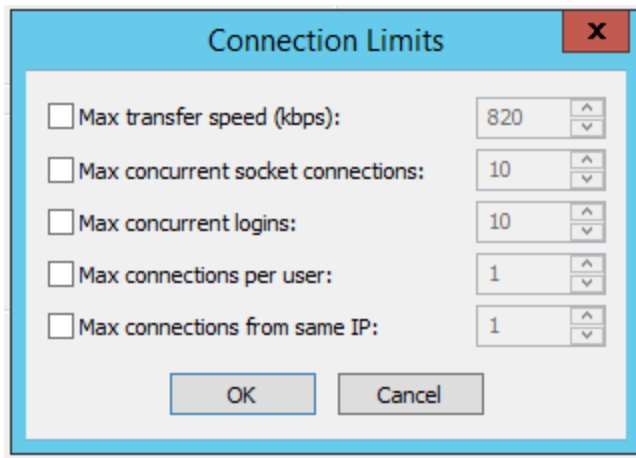
You can set the maximum number of simultaneous connections for a user on the Site, Settings Template, and/or for each user.

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.

- Next to **Connection limits**, click **Configure**. The **Connection Limits** dialog box appears.



- 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.)
- Click **OK** to close the dialog box.
- Click **Apply** to save the changes on EFT.

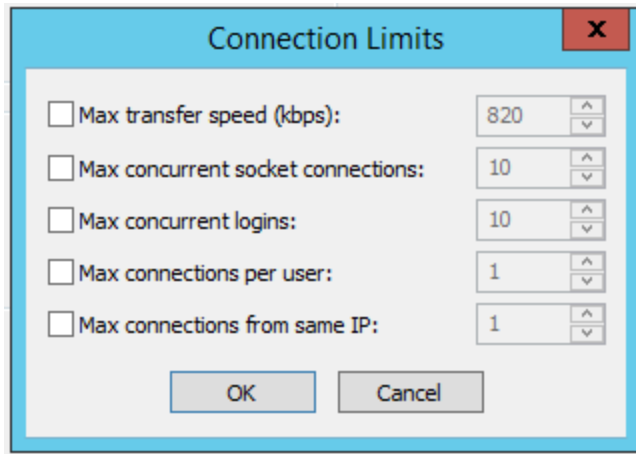
Setting Maximum Connections per IP Address

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

- In the administration interface, [connect to EFT](#) and click the **Server** tab.
- On the **Server** tab, click the Site, Settings Template, or user account that you want to configure.
- In the right pane, click the **Connections** tab.
- Next to **Connection limits**, click **Configure**. The **Connection Limits** dialog box appears.



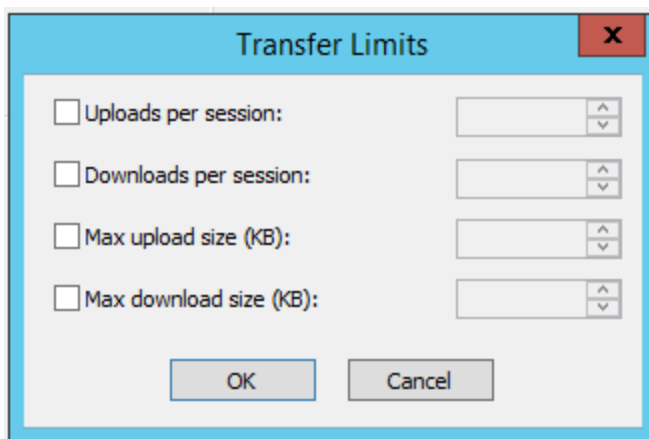
5. Select the **Max connections from same IP** check box and type the maximum number of simultaneous connections you want to allow from the same IP address. (You must specify an integer between 1 and 99999.)
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

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.



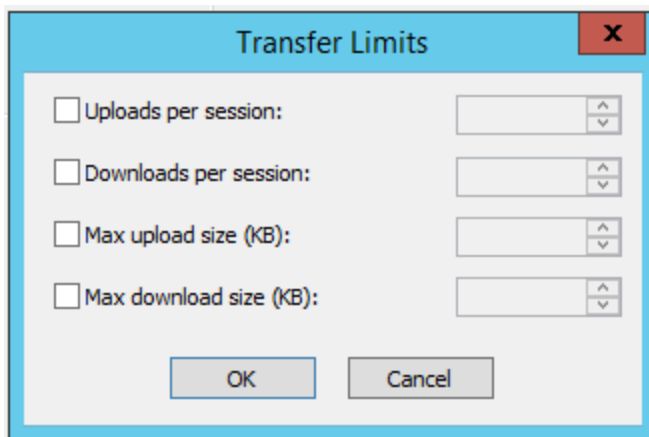
5. Select the **Uploads** and/or **Downloads per session** check box and specify the maximum number of uploads/downloads the user may transfer during a session.
6. Click **OK** to close the dialog box.
7. Click **Apply** to save the changes on EFT.

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.

The image shows a 'Transfer Limits' dialog box with a blue title bar and a red close button. It contains four rows of settings, each with a checkbox and a numeric input field with up/down arrows. The settings are: 'Uploads per session:', 'Downloads per session:', 'Max upload size (KB):', and 'Max download size (KB):'. At the bottom are 'OK' and 'Cancel' buttons.

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.

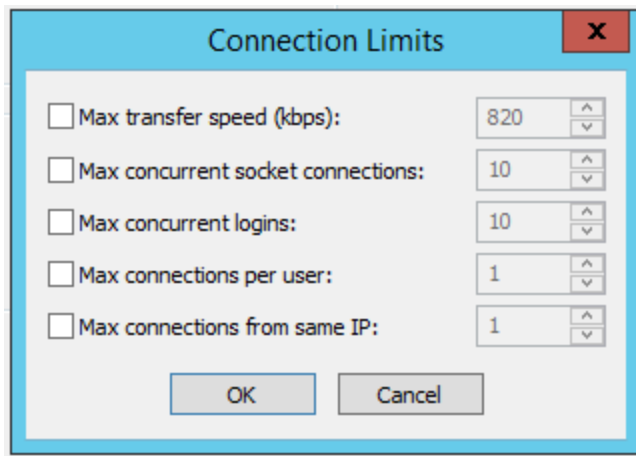
Setting Maximum Transfer Speeds

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.

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\Templates** (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.

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.

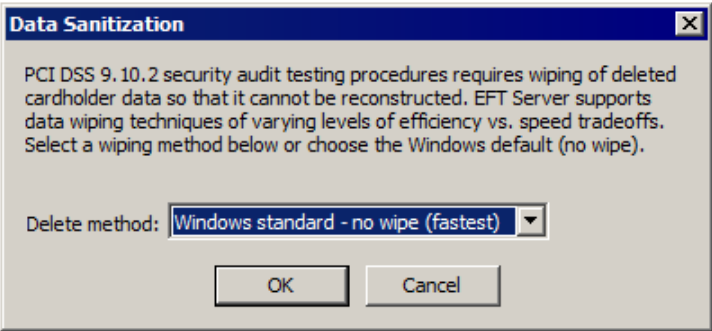
You can configure EFT to securely delete or purge a file by writing over the initial data using encrypted and/or pseudorandom data. A menu of purging methods is available; available options depend on the library used.

- 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	GUI	Usage	Remarks
	(Internal Representation on Disk)	(Allowed and Displayed)		
General				

Area	Storage (Internal Representation on Disk)	GUI (Allowed and Displayed)	Usage	Remarks
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.
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				

Area	Storage (Internal Representation on Disk)	GUI (Allowed and Displayed)	Usage	Remarks
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.
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				

Area	Storage (Internal Representation on Disk)	GUI (Allowed and Displayed)	Usage	Remarks
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 [polling](#) only 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.

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](#).)

The image shows two instances of the 'User Account Details Template' dialog box. Both have a title bar with a close button (X). The left dialog has a drop-down menu showing 'Email' and a table of attributes for that field. The right dialog has a drop-down menu showing 'Comments' and a list of available fields.

Field	Display name	Default value	Is personal data?	Is modifiable?	Is enabled?	Is visible to user?
Email	Email		☒	☒	☒	☒

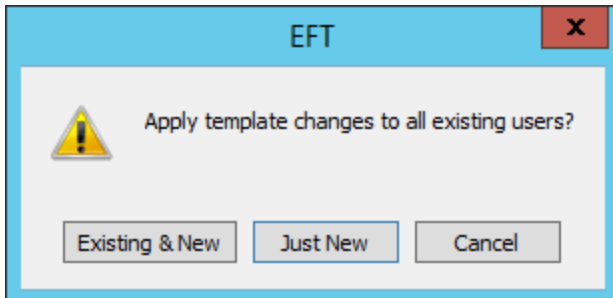
Available fields for 'Comments':

- Email
- Full Name
- Company Name
- Mobile
- Description
- Phone
- Fax
- Pager
- DUNS
- Partner ID
- Custom 1
- Custom 2
- Custom 3
- Comments

To change the user account fields attributes, default value, and display name

- 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 image shows two screenshots of the 'User Account Details' dialog box. The left screenshot is titled 'User Account Details Template' and contains a list of fields with their attributes. The 'Display name' field is highlighted with a red box, and its value is 'Bldg. #'. The right screenshot is titled 'User Account Details for lmauser1' and shows the same fields as the template. The 'Bldg. #' field is highlighted with a red box, and a red arrow points from the 'Display name' field in the template to this field in the user details 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.

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**.

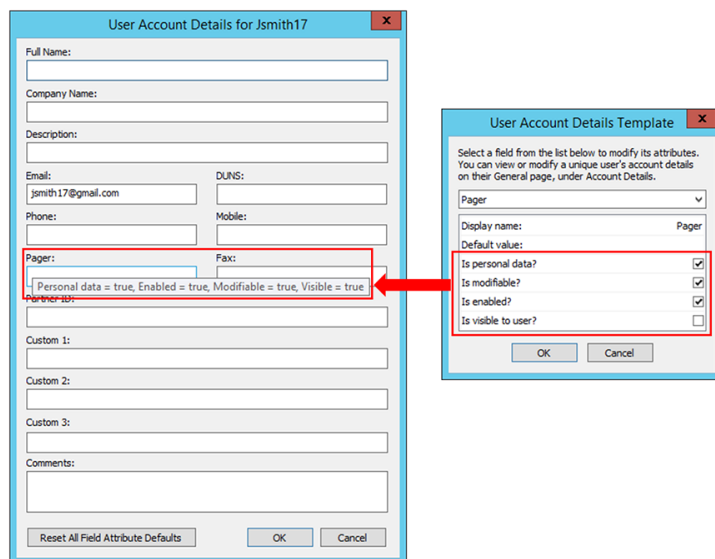
The default setting (true or false) for each field are shown in the table below:

FieldName	Email	Full Name	Company Name	Mobile	Description	Phone	Fax	Pager	DUNS	Partner ID	Custom1	Custom2	Custom3	Comments
Display name	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Is Personal data?	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Is Modifiable?	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Is Enabled?	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
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**

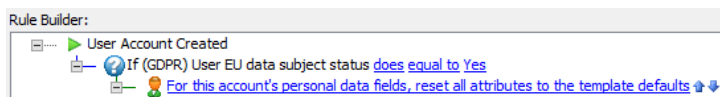
Field Attribute Defaults to make the field attributes in the **User Account Details** dialog box match the template's settings.



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.



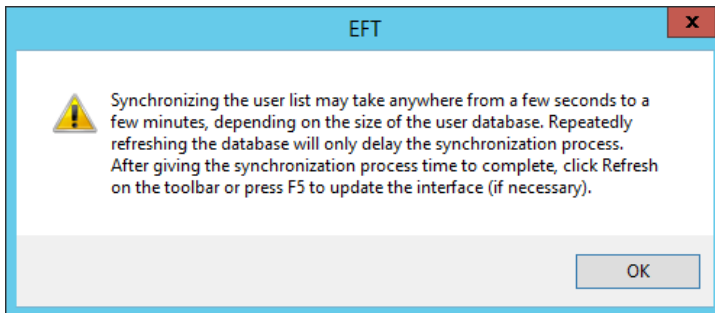
User Database Refresh

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.

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 screenshot shows the 'General' tab of the Site Configuration interface. The 'Site root folder' is set to 'C:\inetpub\efroot\MySite'. The 'User auth manager' is set to 'Globalscape EFT Authentication'. Under 'Advanced Authentication Options', 'None' is selected. The 'Statistics' tab is also visible, showing the site status as 'Running' with a green dot. Other statistics include start date/time, last modified time, active sessions, users defined, workspaces licenses, remote agent licenses, scClient sessions, active uploads/downloads, and average speed.

Statistics	
Site status:	Running  Stop
Start date/time:	Tuesday, October 11, 2022, 14:08:18
Last modified time:	Oct 10, 2022. 10:16:34 AM
Last modified by:	Eftserver1
Active sessions:	0
Users defined:	1
Workspaces licenses:	0 (0 normal, 0 drop-off) assigned / 100 remaining
Remote Agent licenses:	1 Licenses Remaining / 1 Total Licenses
scClient sessions:	0 active / 0 remaining
Active uploads:	0
Active downloads:	0
Average speed:	0 bps

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.

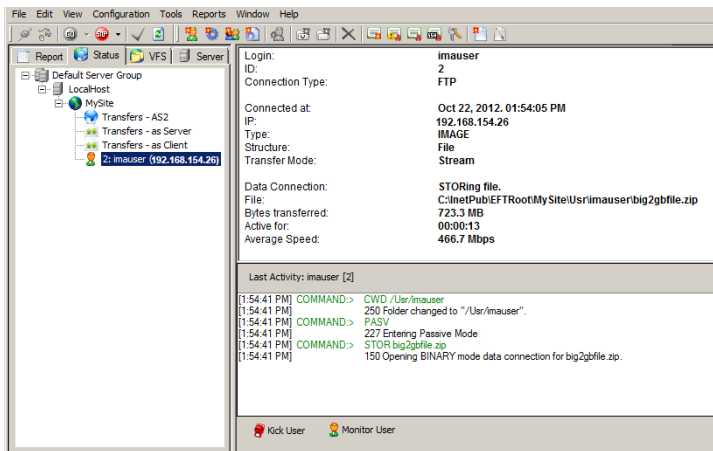
Viewing Connections to a Site

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.

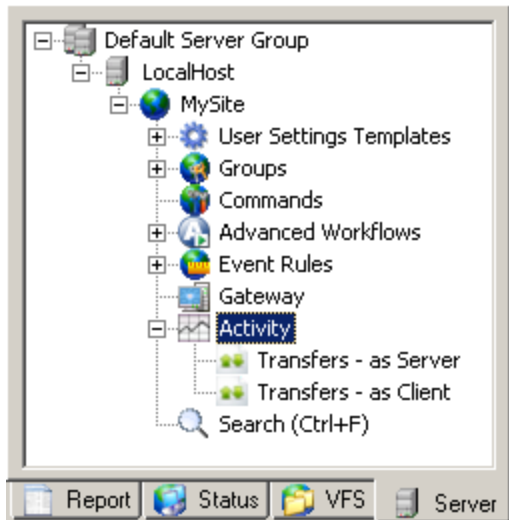
You can [forcibly disconnect a user](#) by selecting the user in the tree, and then clicking **Kick User** in the right pane.

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.

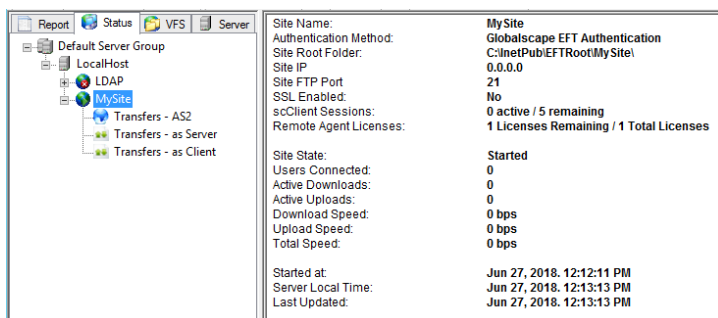


Viewing Transfers To and From a Site

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.

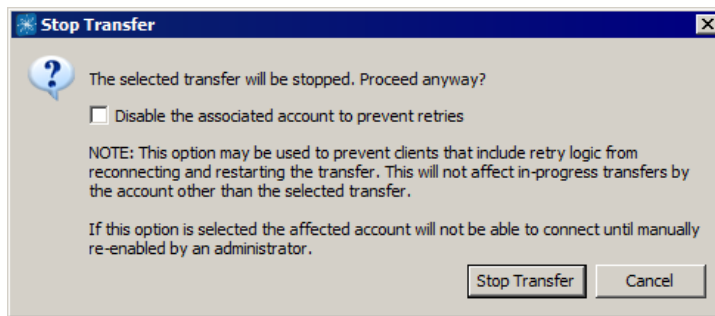
Date/Time	Status	Direction	Username	File Name	Remote IP	Protocol	Path	Transferred	Rate	Elapsed
06/29/09-31:56 AM	Success	Receiving	jobob	winutil	127.0.0.1	HTTPS	C:\Program Files\WinUtil	92 B	736 Bps	00:00:00
06/29/09-31:56 AM	Success	Receiving	jobob	_defaut.pdf	127.0.0.1	HTTPS	C:\Program Files\WinUtil	707 B	6 Bps	00:00:00
06/29/09-31:56 AM	Success	Receiving	jobob	win102.exe	127.0.0.1	HTTPS	C:\Program Files\WinUtil	9 KB	74 Bps	00:00:00
06/29/09-31:56 AM	Success	Receiving	jobob	winhelp.exe	127.0.0.1	HTTPS	C:\Program Files\WinUtil	250 KB	2.0 Mbps	00:00:00
06/29/09-31:56 AM	Success	Receiving	jobob	WindowsUpdate.log	127.0.0.1	HTTPS	C:\Program Files\WinUtil	1.2 MB	10.0 Mbps	00:00:00
06/29/09-29:18 AM	Success	Receiving	jobob	bootstat.dat	127.0.0.1	HTTPS	C:\Program Files\WinUtil	66 KB	541 Bps	00:00:00
06/29/09-29:17 AM	Success	Receiving	jobob	360.exe	127.0.0.1	HTTPS	C:\Program Files\WinUtil	58 KB	472 Bps	00:00:00
06/29/09-29:17 AM	Success	Receiving	jobob	Dtdinstall.log	127.0.0.1	HTTPS	C:\Program Files\WinUtil	2 KB	14 Bps	00:00:00
06/29/09-29:16 AM	Success	Receiving	jobob	explorer.exe	127.0.0.1	HTTPS	C:\Program Files\WinUtil	2.8 MB	13.4 Mbps	00:00:00
06/29/09-29:16 AM	Success	Receiving	jobob	Freeupdate.exe	127.0.0.1	HTTPS	C:\Program Files\WinUtil	13 KB	106 Bps	00:00:00
06/29/09-29:15 AM	Success	Receiving	jobob	msipfame.exe	127.0.0.1	HTTPS	C:\Program Files\WinUtil	487 KB	4.0 Mbps	00:00:00
06/29/09-29:14 AM	Success	Receiving	jobob	Win.exe	127.0.0.1	HTTPS	C:\Program Files\WinUtil	15 KB	119 Bps	00:00:00
06/29/09-29:13 AM	Success	Receiving	jobob	esl_main.log	127.0.0.1	HTTPS	C:\Program Files\WinUtil	2 KB	17 Bps	00:00:00
06/29/09-29:13 AM	Success	Receiving	jobob	ESL_main.log	127.0.0.1	HTTPS	C:\Program Files\WinUtil	4 KB	24 Bps	00:00:00
06/29/09-29:13 AM	Success	Receiving	jobob	is7.log	127.0.0.1	HTTPS	C:\Program Files\WinUtil	74 KB	608 Bps	00:00:00
06/29/09-29:12 AM	Success	Receiving	jobob	mba.bin	127.0.0.1	HTTPS	C:\Program Files\WinUtil	42 KB	345 Bps	00:00:00
06/29/09-29:11 AM	Success	Receiving	jobob	msipfame.exe	127.0.0.1	HTTPS	C:\Program Files\WinUtil	1 KB	11 Bps	00:00:00
06/29/09-29:11 AM	Success	Receiving	jobob	ocsetup_cbs_install_jfied	127.0.0.1	HTTPS	C:\Program Files\WinUtil	32 KB	262 Bps	00:00:00
06/29/09-29:10 AM	Success	Receiving	jobob	nanep.dat	127.0.0.1	HTTPS	C:\Program Files\WinUtil	0 B	0 Bps	00:00:00

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.

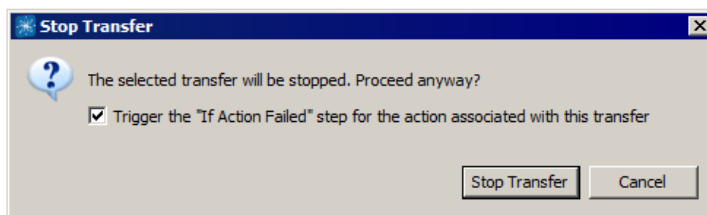
You can:

- 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
Local Port	Server's port on which the file is transferred	x	n/a
Remote Port	Port of remote computer used for transfer	n/a	x
Protocol	Protocol over which the file is transferred	x	x
Path	Path on EFT to which file is transferred	x	n/a
Remote Path	Remote path of file being transferred	n/a	x

Column	Description	Transfers as Server	Transfers as Client																																		
Local Path	Local path of file being transferred	n/a	x																																		
Transferred	Size of file being transferred	x	x																																		
% Complete	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>	Protocol	EFT as server		EFT as client (that is, Event Rules)		Inbound (client push to server)	Outbound (client pull from server)	Outbound (EFT pushing to client)	Inbound (EFT pulling from client)	HTTP	%	%	%	%	HTTPS	%	%	%	%	FTP	n/a	%	%	%	FTPS	n/a	%	%	%	SFTP	n/a	n/a	%	%	x	x
Protocol	EFT as server		EFT as client (that is, Event Rules)																																		
	Inbound (client push to server)	Outbound (client pull from server)	Outbound (EFT pushing to client)	Inbound (EFT pulling from client)																																	
HTTP	%	%	%	%																																	
HTTPS	%	%	%	%																																	
FTP	n/a	%	%	%																																	
FTPS	n/a	%	%	%																																	
SFTP	n/a	n/a	%	%																																	
Rate	Rate, in kilobits per second (kbps), at which the file is transferred	x	x																																		
Elapsed	Time in HH:MM:SS that it took to transfer the file	x	x																																		

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

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](#).

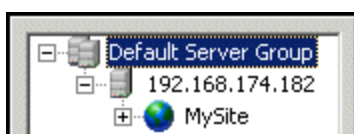
This procedure is for installing only the administration interface on a computer that is remote from EFT.

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."

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.

The screenshot displays the EFT Administration interface with the 'Administration' tab selected. The 'Server Administration Connectivity' section is highlighted with a red box, showing the following options:

- ☒ Allow remote administration
- ☒ Enable REST API / web admin
- REST API / web admin port: 4450
- ☒ Require SSL for remote administration: [Configure](#)
- IP ban/access list for remote administration: [Configure](#)

The 'Administrator Access and Permissions' section is also highlighted with a red box, showing the following options:

- Selected account permissions policy: Server Admin(full control)
- Optional permissions: ☒ Run & Edit Reports, ☒ COM (programmatic control), ☒ Manage personal data, ☐ Web Admin Client
- Assigned to this server: [Empty list box]
- ☒ Programmatic API Policy: server_full_access

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.

- 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."

- 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.

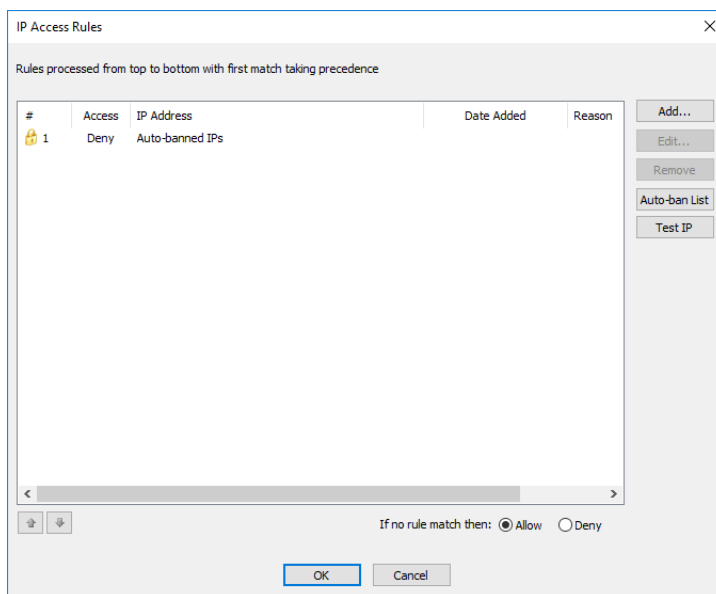
IP Access Rules for Remote Administration

By default, all IP addresses are granted remote access to EFT. EFT allows you to grant [remote administration](#) 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. Refer to [Controlling Access to the Site by IP Address](#) for details of banning IP addresses.

To grant/deny access by IP address

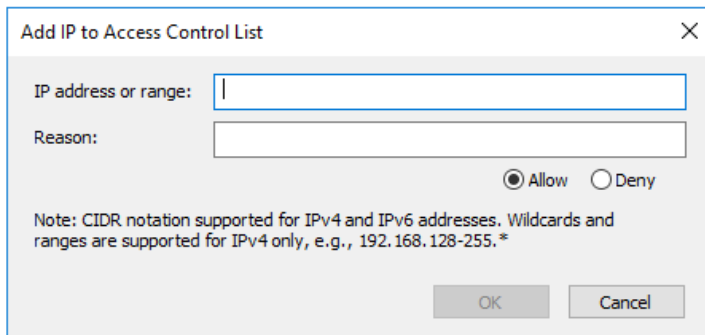
- In the administration interface, [connect to EFT](#) and click the **Server** tab.
- On the **Server** tab, click the Server node that you want to configure.
- In the right pane, click the **Administration** tab.
- Select the **Allow remote administration** check box.
- Next to **IP ban/access list 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.



The dialog box titled "Add IP to Access Control List" contains the following elements:

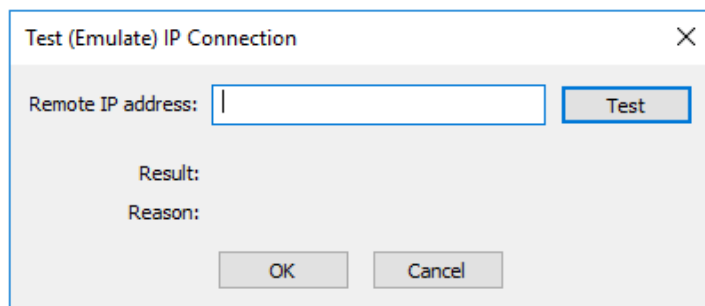
- A text input field labeled "IP address or range:".
- A text input field labeled "Reason:".
- Two radio buttons: "Allow" (selected) and "Deny".
- A note: "Note: CIDR notation supported for IPv4 and IPv6 addresses. Wildcards and ranges are supported for IPv4 only, e.g., 192.168.128-255.*"
- "OK" and "Cancel" buttons at the bottom.

- Specify the IP address or mask.
- Provide a reason for allowing or denying the IP access. (optional)
- Click whether to **Allow** or **Deny** the address.
- 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.

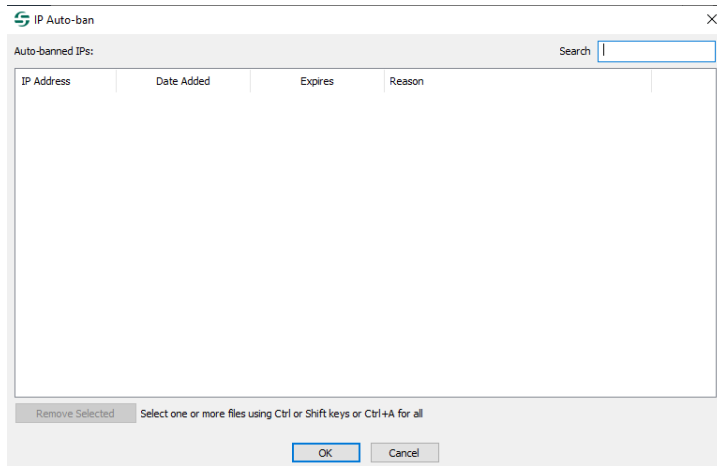


The dialog box titled "Test (Emulate) IP Connection" contains the following elements:

- A text input field labeled "Remote IP address:".
- A "Test" button next to the input field.
- Labels for "Result:" and "Reason:" below the input field.
- "OK" and "Cancel" buttons at the bottom.

- 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.

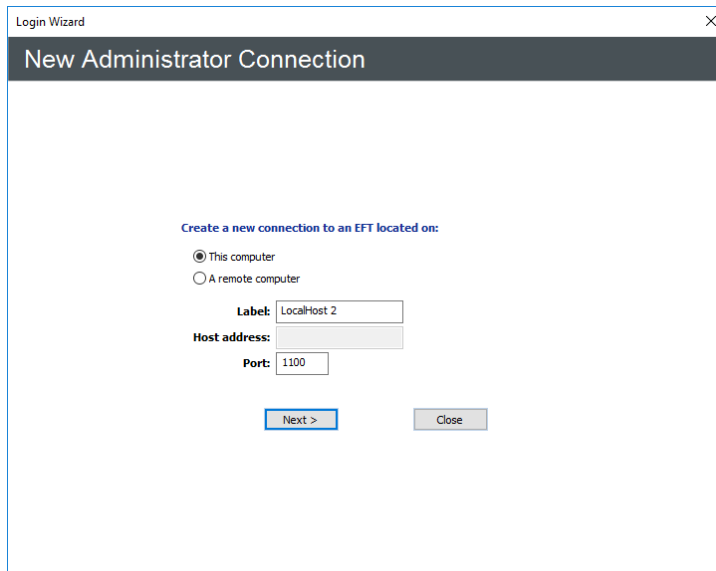
- The **IP Address** column lists the banned IP addresses.
 - The **Date Added** column displays the date and time the IP address was automatically banned, in MM/DD/YYYY hh:mm:ss AM/PM format.
 - The **Reason** column displays the reason the IP address was automatically banned (for example, DoS/Flood 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.

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.



The screenshot shows a window titled 'Login Wizard' with a sub-header 'New Administrator Connection'. The main content area contains the text 'Create a new connection to an EFT located on:' followed by two radio buttons: 'This computer' (selected) and 'A remote computer'. Below these are three input fields: 'Label' with the value 'localhost 2', 'Host address' (empty), and 'Port' with the value '1100'. At the bottom are two buttons: 'Next >' and 'Close'.

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.

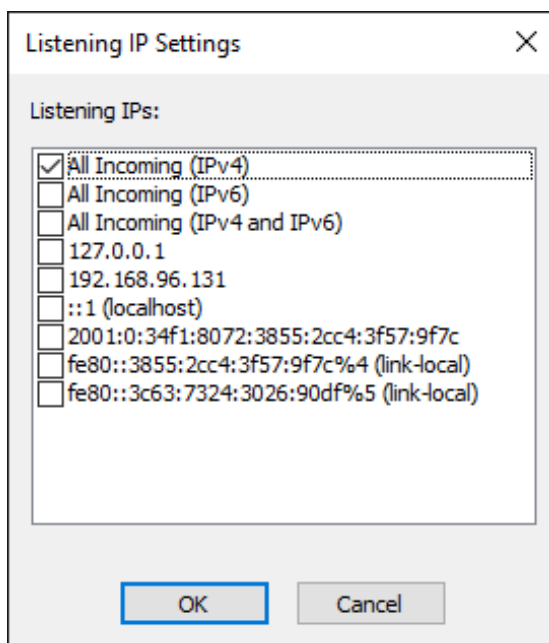
- To use FIPS for SFTP (SSH2), select the **Enable FIPS for SFTP** check box.
- To use FIPS for SSL, select the **Enable FIPS for SSL** check box.
- A confirmation prompt appears when you select either check box. When you enable FIPS, the EFT service must be restarted. Click **OK** to continue with FIPS 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.

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.

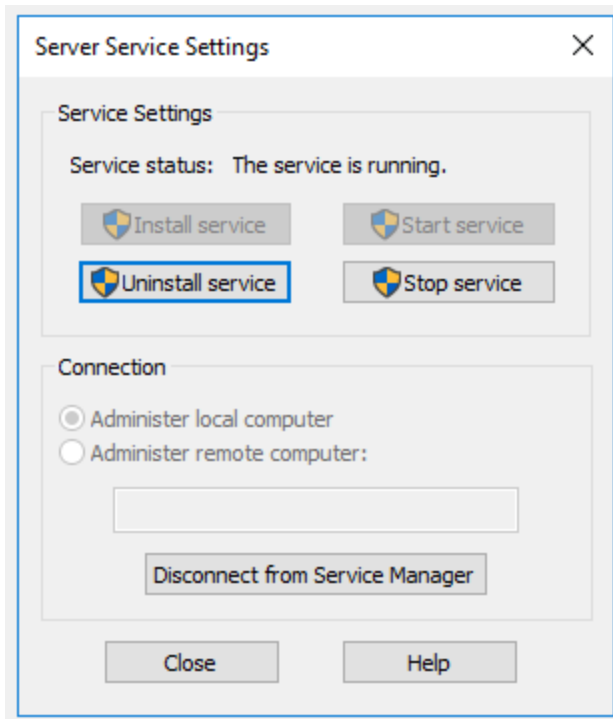
Starting and Stopping EFT Remotely

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.



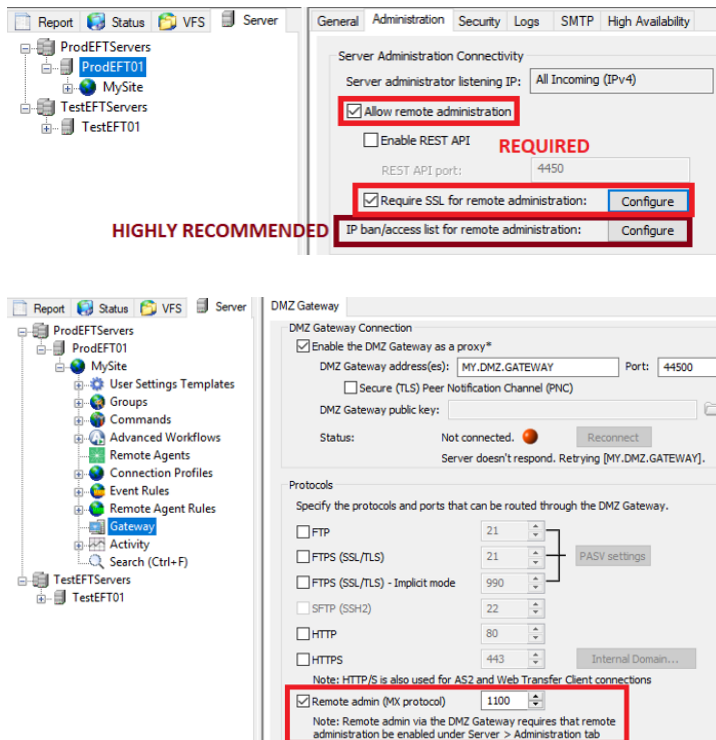
2. In the **Connection** area, select **Administer remote computer**.
3. In the text box, type or paste the IP address of the server you want to administer.
4. Click **Connect to Service Manager**.
5. Click **Start service** (or **Stop service**) and close the **Server Service Settings** dialog box.

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-key> for 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** file 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**)

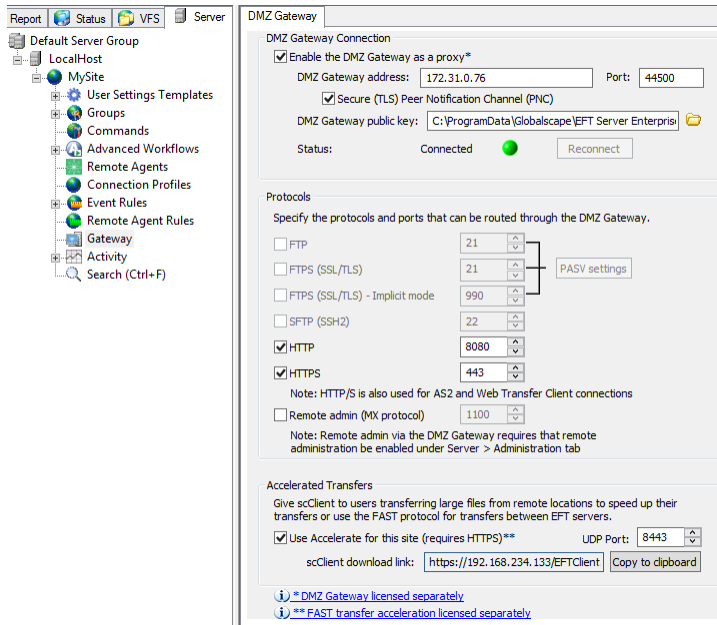
NOTE: You must enter the proper XML format for these values otherwise the service will not start, e.g.,

```
<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.

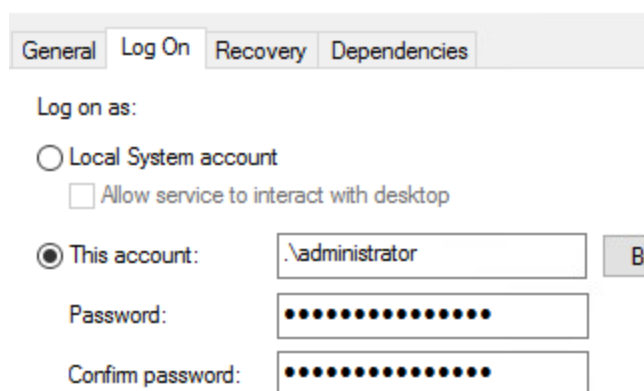
If the **SecurePNCEnabled** setting is set to true, then it also acts like a “require SSL” setting in that only secure peer notification channels will be allowed. In other words, whether or not a channel is to be secured is enforced by the server and not solely dictated by the client.

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>AllIPs</AccelerationIP>
<SecurePNCEnabled>true</SecurePNCEnabled>
<PNCKeyStorePath>\\192.168.100.143\keystore\keystore.jks</PNCKeyStorePath>
<PNCTrustStorePath>\\192.168.100.143\keystore\truststore.jks</PNCTrustStorePath>
<PNCStorePassphrase>OSB8j8m8s8080x130eq8roJ2DrQok81731Y190hUx6Jq8vm508P0d3aVaqJ1o1ByoqYxy8gD2R157b42aa5f2Ttg=</PNCStorePassphrase>
<PNCProtocols>TLSv1.2,TLSv1.1</PNCProtocols>
<PNCciphers>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_EC
```

DMZ Gateway Server Properties (Local Computer)



Log on as:

☐ Local System account

☐ Allow service to interact with desktop

☒ This account:

Password:

Confirm password:

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
- SSLv2Hello

PNCiphers – 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.

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</PNCTrustStorePath>

<PNCStorePassphrase>GSBEvsavuSo9cA60O18fS5B+ubI+zdoDBYTzMoA3vtDQiiA65
hLnVLdRAwyIZStqezbpLnbsu3E1IOH5Fh1Hij9qjQ==</PNCStorePassphrase>
<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>
```

Database Authentication Types

The topics below provide information regarding specifying the user database to use for Site 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.

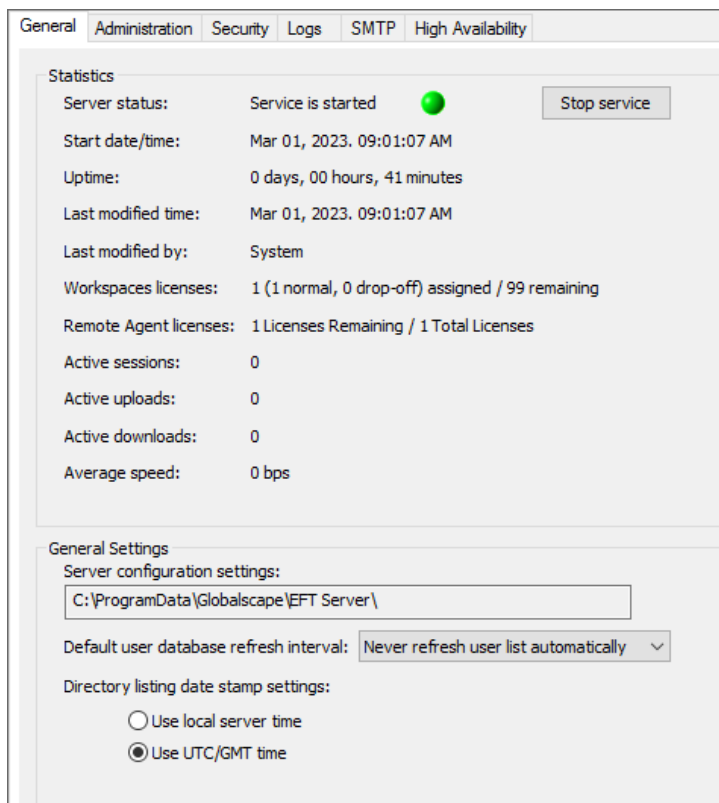
Database refresh should be disabled on EFT nodes used in HA configurations. (Set to **Never refresh user list automatically.**)

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**.

Active Directory Authentication

The topics below provide information about AD authentication on EFT.

Local Security Policy Setting when Using Active Directory Authentication

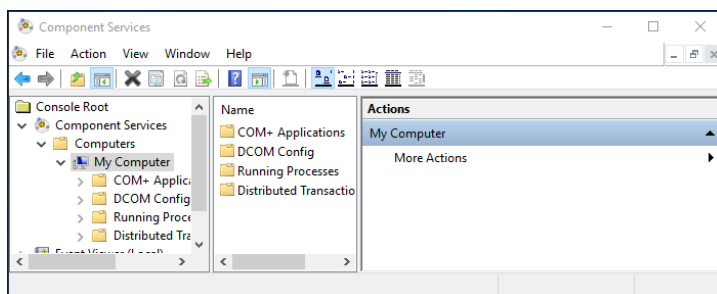
To use AD authentication, Globalscape Customer Support recommends creating an AD account for the EFT service "Log on as" account with adequate privileges to all of the resources (AD domain query, network shares) required for the Site. There is no set formula for the type of account needed, because network 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:

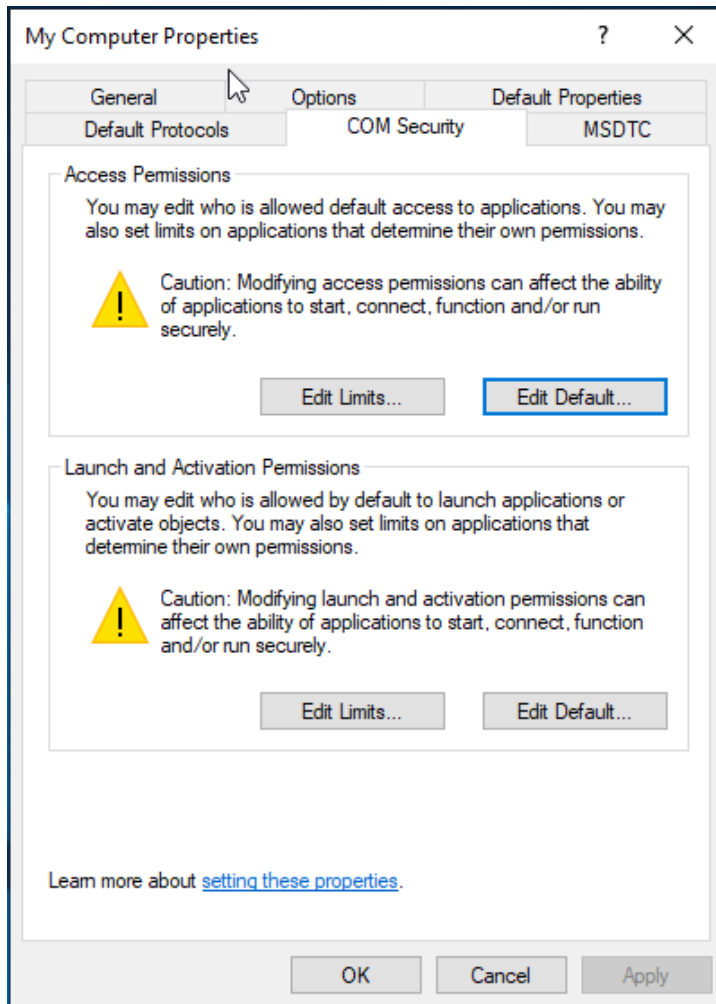
- Installation folder
- Application data folder
- Windows temp folder (varies by system)
- Any shared drive paths required by EFT
- Any output directories to which EFT may need to read/write files

In **Component Services**, provide the appropriate permissions:

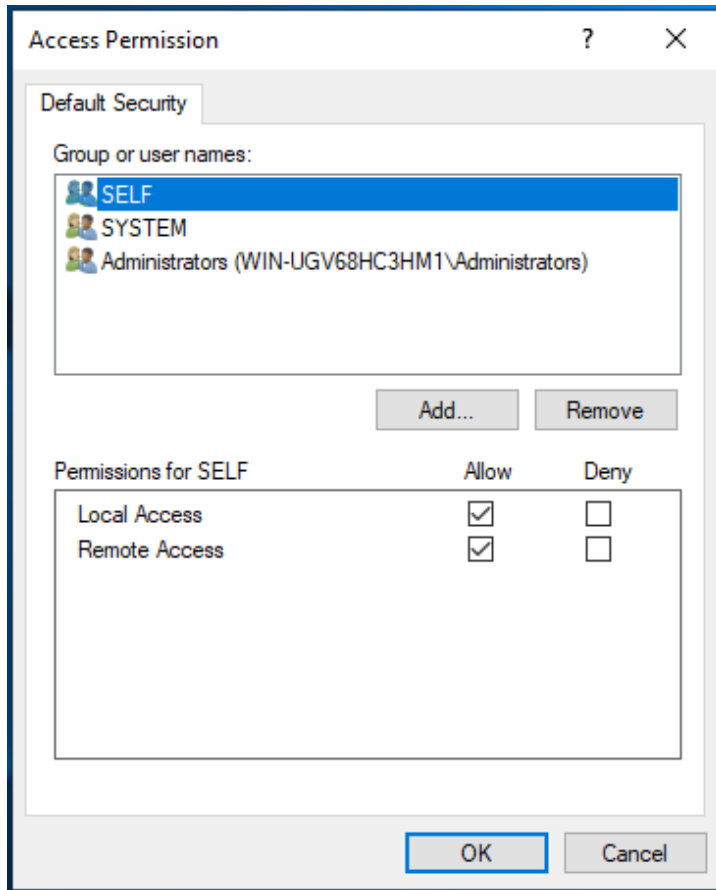
1. Click **Start > Run**, type **dcomcnfg.exe**, then press ENTER. **Component Services** appears.
2. Expand **Component Services > Computers**.



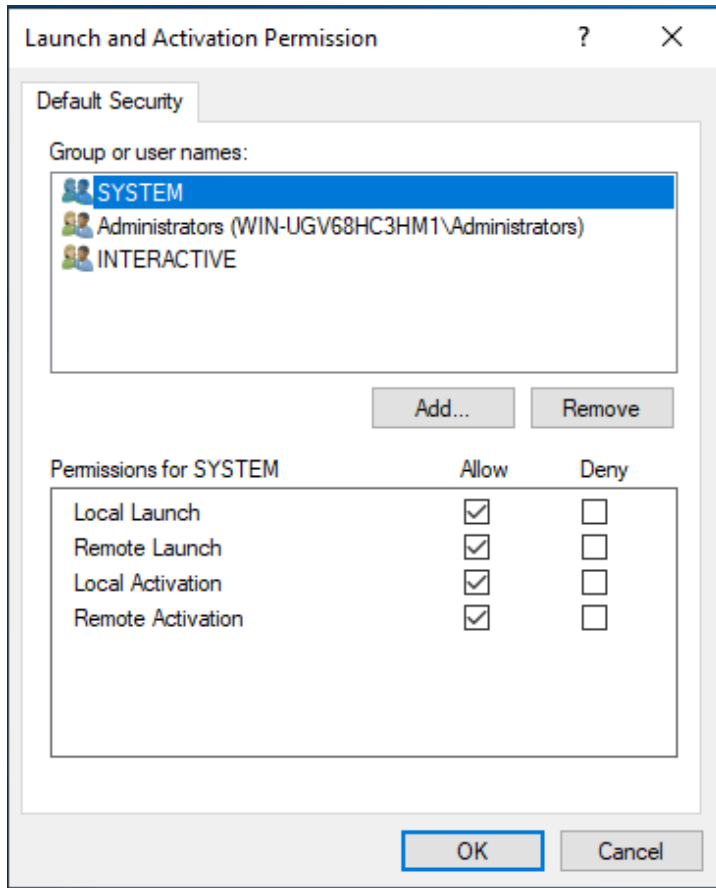
3. Right-click the **My Computer** node, and then click **Properties**. The **My Computer Properties** dialog box appears.



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.

EFT Site Setup Wizard

Windows Authentication Options

Type: ☒ Active Directory ☐ Local System Accounts

Domain: ☒ Default ☐ Specify:

Group: ☒ Everyone ☐ Specify:

Separate multiple groups by using a comma.
E.g. Accounting, Sales.

Advanced

Use this user attribute as account name:

User list refresh interval:

☐ Synchronize user(s) only after they first attempt to log in

☒ Access permissions are managed by Windows

When creating home folders for newly added users:

☐ Create a virtual folder pointing to the user's home folder as defined in his/her AD profile

☐ Keep user's home folder in sync with AD profile folder

☒ Create a physical folder under the site root folder using the user's login name

☐ Don't include domain attribute in folder name, e.g. /jsmith, rather than /domain.jsmith

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.

Windows Authentication Options

Type: ☒ Active Directory ☐ Local System Accounts

Domain: ☒ Default ☐ Specify:

Group: ☒ Everyone ☐ Specify:

Separate multiple groups by using a comma.
E.g. Accounting, Sales.

Advanced

Use this user attribute as account name:

☐ Refresh user list automatically every minutes

Note: Not required. User list will update when user attempts to connect and is authenticated against the active directory server.

☐ Synchronize user(s) only after they first attempt to log in

When creating home folders for newly added users:

☐ Create a virtual folder pointing to the user's home folder as defined in his/her AD profile

☐ Keep user's home folder in sync with AD profile folder

☒ Create a physical folder under the site root folder using the user's login name

☐ Don't include domain attribute in folder name, e.g. /jsmith, rather than /domain.jsmith

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
☒	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.

Windows Authentication Options

Type: ☒ Active Directory ☐ Local System Accounts

Domain: ☒ Default ☐ Specify:

Group: ☒ Everyone ☐ Specify:

Test

Separate multiple groups by using a comma.
E.g. Accounting, Sales.

Advanced

Use this user attribute as account name:

☐ Refresh user list automatically every minutes

Note: Not required. User list will update when user attempts to connect and is authenticated against the active directory server.

☐ Synchronize user(s) only after they first attempt to log in

When creating home folders for newly added users:

☐ Create a virtual folder pointing to the user's home folder as defined in his/her AD profile

☐ Keep user's home folder in sync with AD profile folder

☒ Create a physical folder under the site root folder using the user's login name

☐ Don't include domain attribute in folder name, e.g. /jsmith, rather than /domain.jsmith

OK **Cancel** **Help**

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

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.

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 194](#), 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 194](#) or editing the [LDAP authentication options](#).

More examples:

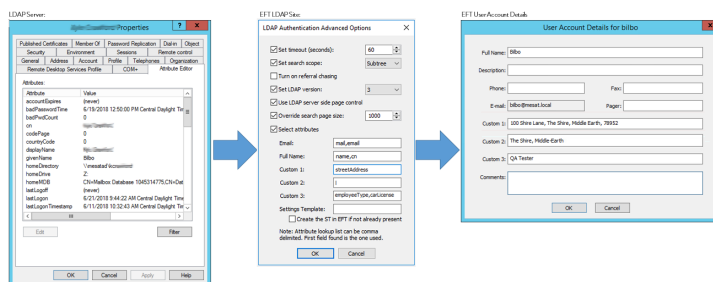
Search filter	Description
(objectClass=*)	All objects
(&(objectCategory=person)(objectClass=user)(!cn=andy))	All user objects but "andy"
(sn=sm*)	All objects with a surname that starts with "sm"
(&(objectCategory=person)(objectClass=contact)(!(sn=Smith)(sn=Johnson)))	All contacts with a surname equal 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**.

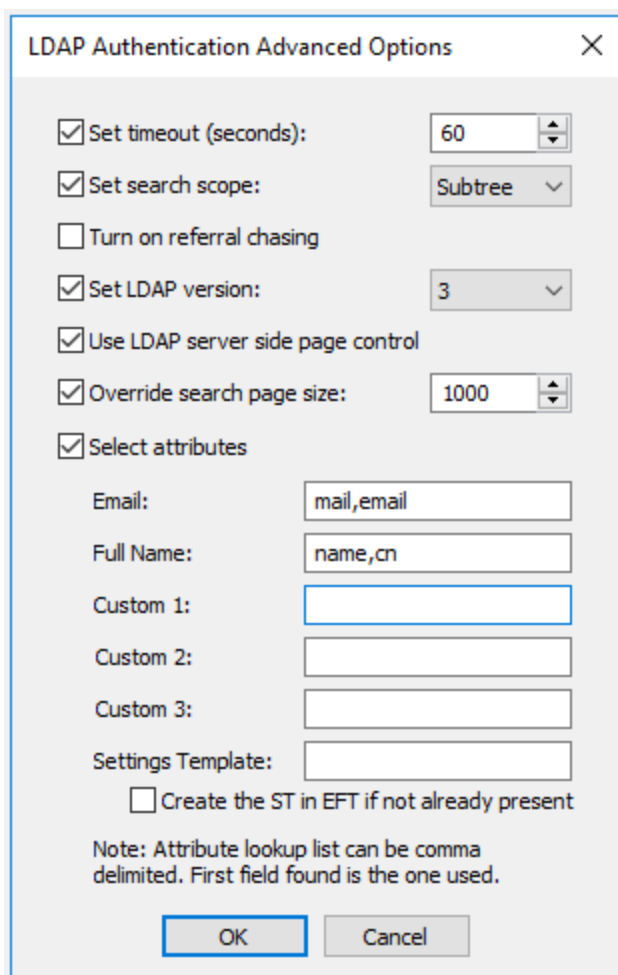


To map LDAP attributes to EFT user accounts

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.



The image shows a dialog box titled "LDAP Authentication Advanced Options" with a close button (X) in the top right corner. The dialog contains several configuration options:

- ☒ Set timeout (seconds): 60 (spin box)
- ☒ Set search scope: Subtree (dropdown)
- ☐ Turn on referral chasing
- ☒ Set LDAP version: 3 (dropdown)
- ☒ Use LDAP server side page control
- ☒ Override search page size: 1000 (spin box)
- ☒ Select attributes
 - Email: mail,email (text box)
 - Full Name: name,cn (text box)
 - Custom 1: (empty text box)
 - Custom 2: (empty text box)
 - Custom 3: (empty text box)
 - Settings Template: (empty text box)
- ☐ Create the ST in EFT if not already present

At the bottom, there is a note: "Note: Attribute lookup list can be comma delimited. First field found is the one used." and two buttons: "OK" and "Cancel".

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.)

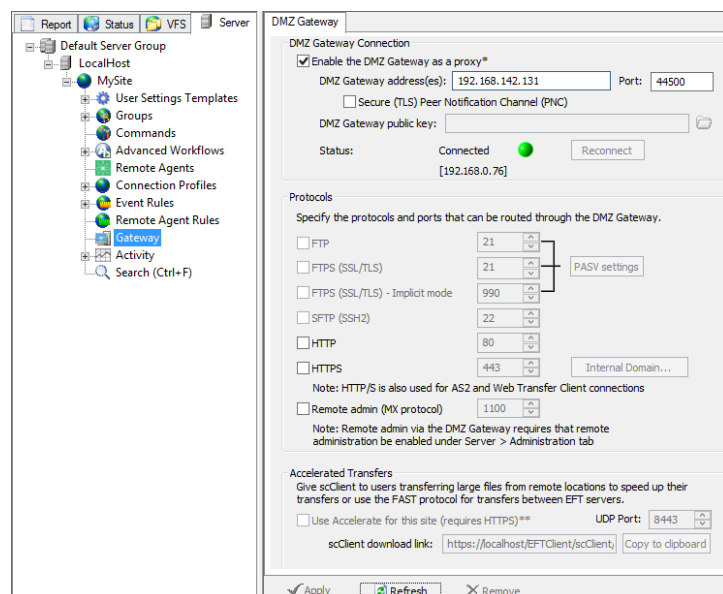
Hyperlinks in Workspaces notification emails are composed **based upon recipient domain**:

- 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:

The screenshot shows the 'Connections' tab of a configuration window. The 'Listener Settings' section is active, displaying options for listening IP addresses and protocols. The 'Listening IP addresses' dropdown is set to 'All Incoming (IPv4)'. Below this, several protocols are listed with checkboxes and associated ports: FTP (21), FTPS (SSL / TLS) - Explicit mode* (21), FTPS (SSL / TLS) - Implicit mode* (990), SFTP (SSH2)* (22), HTTP* (80), and HTTPS (SSL)* (443). Each protocol has a corresponding 'Configure' button. The 'Domain' field is set to 'localhost'. Other settings include 'AS2*' with an 'AS2 Config' button, 'Require additional factor for HTTP/S auth:*' with a dropdown set to 'OTP - Email delivery' and an 'SMS Config' button, 'Allow Globalscape Mobile Transfer Client (MTC) over HTTPS' with a 'Configure' button, 'Event Rule invoke over WS/SOAP (uses HTTPS port)*', 'Redirect all plaintext HTTP traffic to HTTPS*', 'Enable HSTS', and 'Enable Proxy Protocol for all protocols enabled on this Site'. The 'SSL certificate settings' and 'SSL security settings' sections each have a 'Configure' button. The 'Network Usage and Security Settings' section at the bottom includes 'Connection limits:', 'IP access/ban list:', and 'Denial of Service settings:', each with a 'Configure' button.

An **Internal Domain** is specified on the **DMZ Gateway** tab:

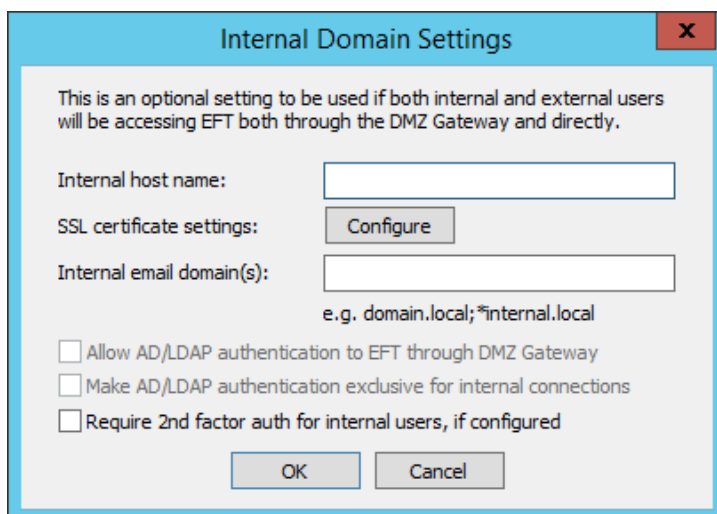


Hyperlinks in notification emails are composed based upon recipient domain

- 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.



Internal Domain Settings

This is an optional setting to be used if both internal and external users will be accessing EFT both through the DMZ Gateway and directly.

Internal host name:

SSL certificate settings:

Internal email domain(s):
e.g. domain.local; *internal.local

☐ Allow AD/LDAP authentication to EFT through DMZ Gateway

☐ Make AD/LDAP authentication exclusive for internal connections

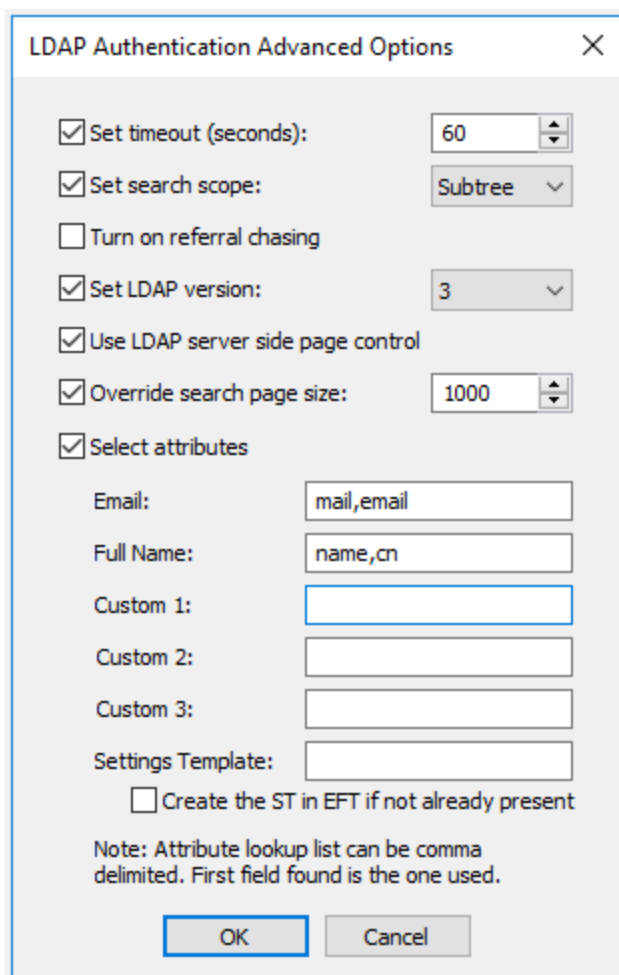
☐ Require 2nd factor auth for internal users, if configured

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.



The dialog box titled "LDAP Authentication Advanced Options" contains the following settings:

- ☒ Set timeout (seconds): 60
- ☒ Set search scope: Subtree
- ☐ Turn on referral chasing
- ☒ Set LDAP version: 3
- ☒ Use LDAP server side page control
- ☒ Override search page size: 1000
- ☒ Select attributes
 - Email: mail,email
 - Full Name: name,cn
 - Custom 1:
 - Custom 2:
 - Custom 3:
 - Settings Template:
- ☐ Create the ST in EFT if not already present

Note: Attribute lookup list can be comma delimited. First field found is the one used.

Buttons: OK, Cancel

Custom Attributes:

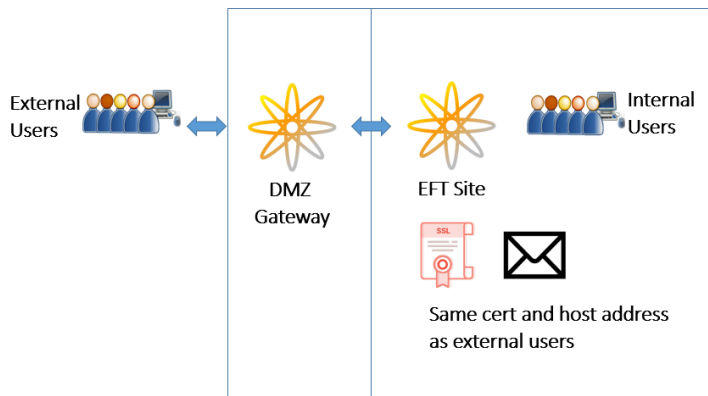
- Multiple attributes can be added to each custom field, but only the first attribute will be used; All other attributes will be ignored
- An attribute field on the AD/LDAP server can contain multiple attributes if you want multiple attributes added to a single custom field (example: address)

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.

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.

The screenshot shows the 'Internal Domain Settings' dialog box. The title bar is blue with a red close button. The main area has a light blue background. It contains the following elements:

- A text block: "This is an optional setting to be used if both internal and external users will be accessing EFT both through the DMZ Gateway and directly."
- A text label "Internal host name:" followed by a text input field.
- A text label "SSL certificate settings:" followed by a "Configure" button.
- A text label "Internal email domain(s):" followed by a text input field. Below the field is the example text "e.g. domain.local; *internal.local".
- Three checkboxes:
 - ☐ Allow AD/LDAP authentication to EFT through DMZ Gateway
 - ☐ Make AD/LDAP authentication exclusive for internal connections
 - ☐ Require 2nd factor auth for internal users, if configured
- At the bottom, "OK" and "Cancel" buttons.

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:

The screenshot shows the 'Connections' tab of the EFT Site configuration. Under 'Listener Settings', various protocols are listed with their respective ports. The 'Domain' field for the HTTPS (SSL) port (443) is highlighted with a red box and contains the value '192.168.100.129'. Other protocols like FTP, FTPS, SFTP, HTTP, and AS2 are also listed with their ports and configuration buttons.

An **Internal Domain** button is available next to the **HTTPS** port box on the **DMZ Gateway** tab of the EFT Site:

The screenshot shows the 'DMZ Gateway' tab of the EFT Site configuration. The 'Internal Domain...' button is highlighted with a red box. The 'Internal Domain Settings' dialog box is open, showing fields for 'Internal host name', 'SSL certificate settings', and 'Internal email domain(s)'. The dialog box also includes checkboxes for 'Allow AD/LDAP authentication to EFT through DMZ Gateway', 'Make AD/LDAP authentication exclusive for internal connections', and 'Require 2nd factor auth for internal users, if configured'.

To specify the internal domain on a site

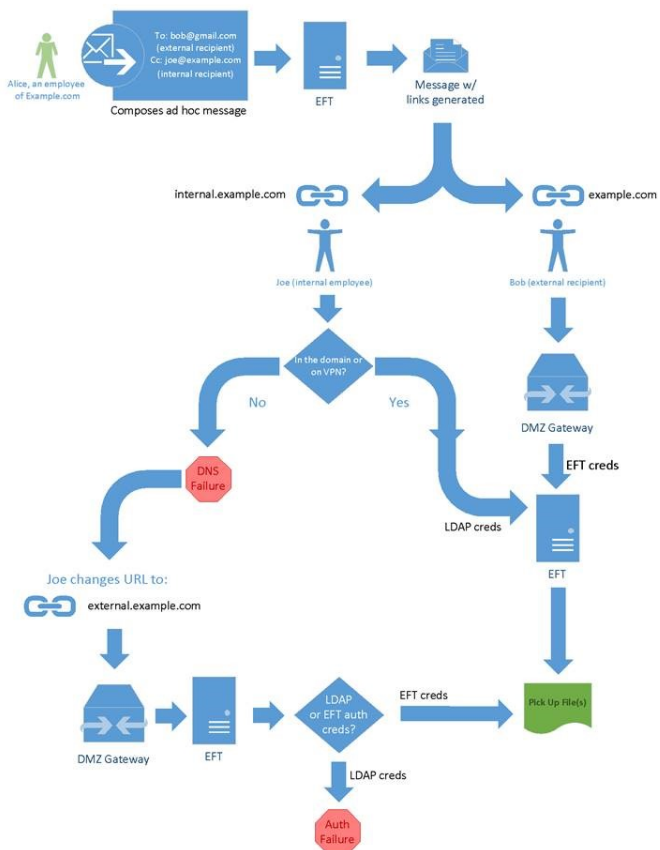
1. In the EFT administration interface, click the **Server** tab, then click the **Gateway** node.
2. On the **DMZ Gateway** tab, next to the **HTTPS** port box, click **Internal Domain**. The **Internal Domain Settings** dialog box appears.
3. In the **Internal host name** box, specify the URL through 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.

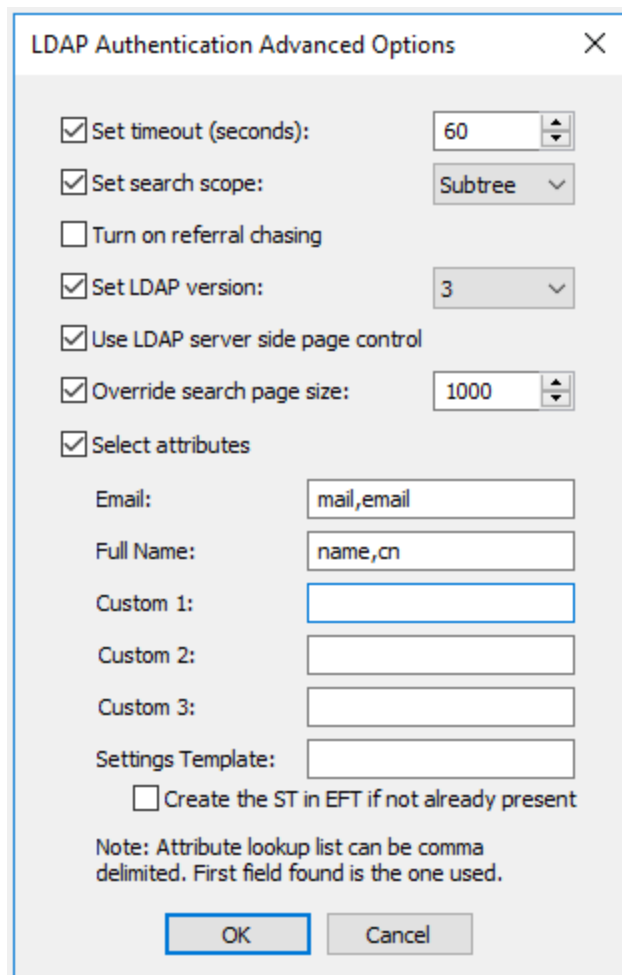


Map LDAP Users to a Settings Template

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**.



The dialog box is titled "LDAP Authentication Advanced Options" and contains the following settings:

- ☒ Set timeout (seconds): 60
- ☒ Set search scope: Subtree
- ☐ Turn on referral chasing
- ☒ Set LDAP version: 3
- ☒ Use LDAP server side page control
- ☒ Override search page size: 1000
- ☒ Select attributes
 - Email: mail,email
 - Full Name: name,cn
 - Custom 1:
 - Custom 2:
 - Custom 3:
 - Settings Template:
- ☐ Create the ST in EFT if not already present

Note: Attribute lookup list can be comma delimited. First field found is the one used.

Buttons: OK, Cancel

(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 DN's from the LDAP server on the domain specified or the default domain. Click **List DN's** 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.

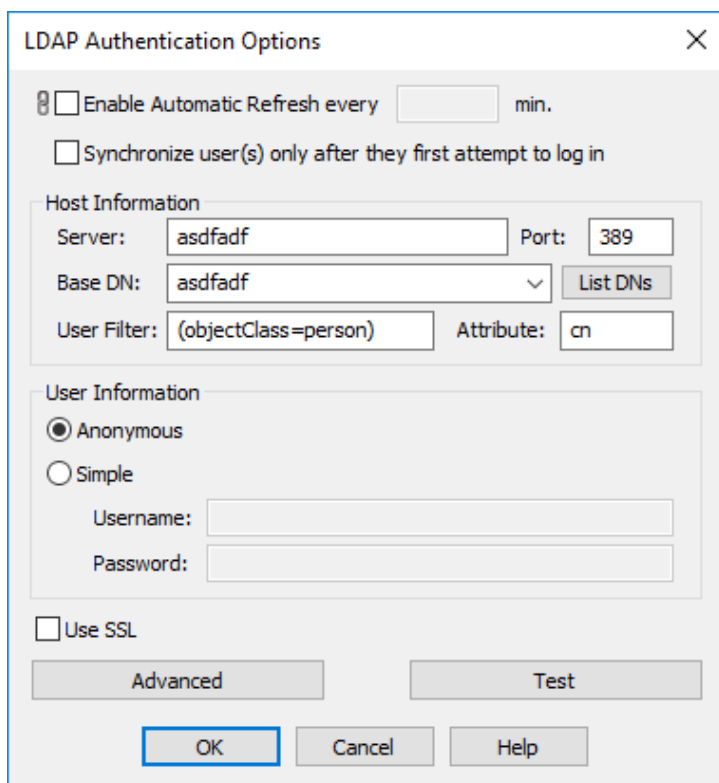
When you use LDAP as the authentication method, EFT pulls the user account list and the authentication from the LDAP Server. Group lists, Group membership, VFS Groups, and VFS User permissions are handled by EFT. These permissions must be configured and maintained in the administration interface or through 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.



The image shows a dialog box titled "LDAP Authentication Options" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Refresh Options:**
 - ☐ Enable Automatic Refresh every min.
 - ☐ Synchronize user(s) only after they first attempt to log in
- Host Information:**
 - Server: Port:
 - Base DN:
 - User Filter: Attribute:
- User Information:**
 - ☒ Anonymous
 - ☐ Simple
 - Username:
 - Password:
- ☐ Use SSL
-
-

- 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.

- 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.
- In the **Server** box, type the **Server** name or IP address.
- 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:

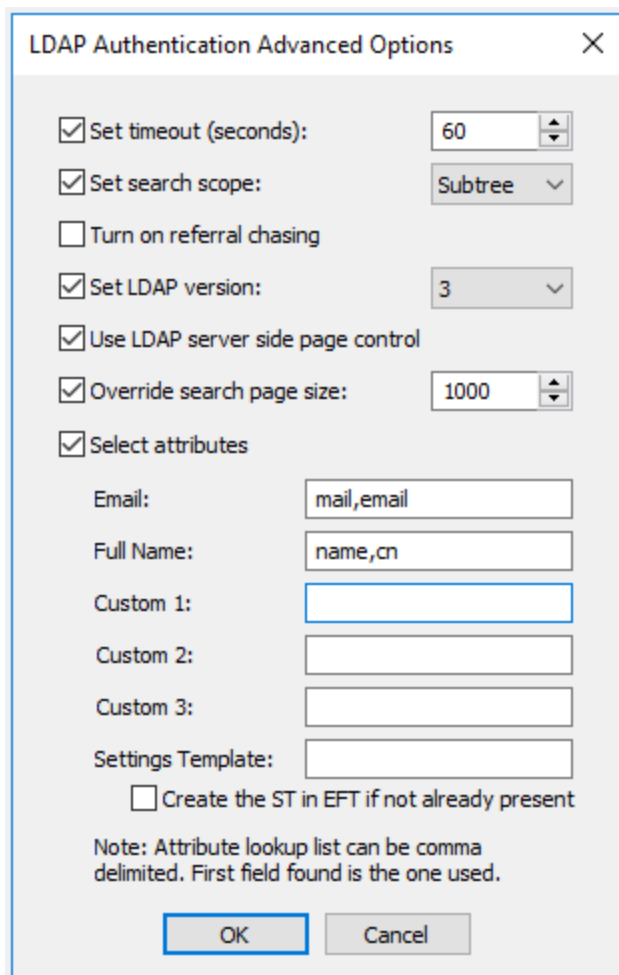
```
cn=Manager,dc=forest,dc=tree,dc=branch
```

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.



The image shows a dialog box titled "LDAP Authentication Advanced Options" with a close button (X) in the top right corner. The dialog contains several configuration options:

- ☒ Set timeout (seconds): 60 (spin box)
- ☒ Set search scope: Subtree (dropdown menu)
- ☐ Turn on referral chasing
- ☒ Set LDAP version: 3 (dropdown menu)
- ☒ Use LDAP server side page control
- ☒ Override search page size: 1000 (spin box)
- ☒ Select attributes
 - Email: mail,email (text box)
 - Full Name: name,cn (text box)
 - Custom 1: (empty text box)
 - Custom 2: (empty text box)
 - Custom 3: (empty text box)
 - Settings Template: (empty text box)
- ☐ Create the ST in EFT if not already present

Below these options is a note: "Note: Attribute lookup list can be comma delimited. First field found is the one used." At the bottom are "OK" and "Cancel" buttons.

- **Set timeout for 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

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=mypassw
ord
```

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.

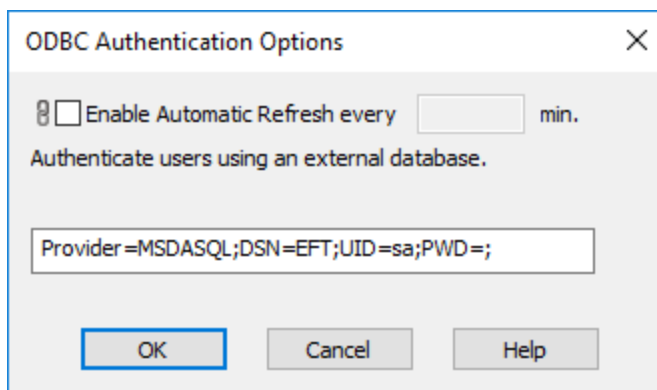
With some installations, you may need to add a pointer to a Microsoft Access workgroup file as well as the username and password. A default installation of Access does not require this.

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.

- 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.

- Click **OK** to close the dialog box.
- 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 "ftpsrvr_users" table is set to "0" or "1"; it cannot be set to "Null".

The **ftpsrvr_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

Field Name	Data Type	Field Size	Description
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.
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.

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.

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.

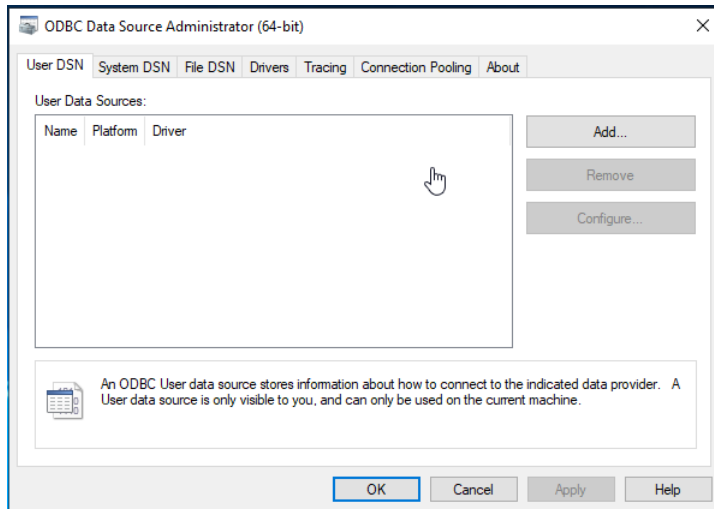
Establishing a System Data Source Name (DSN)

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.

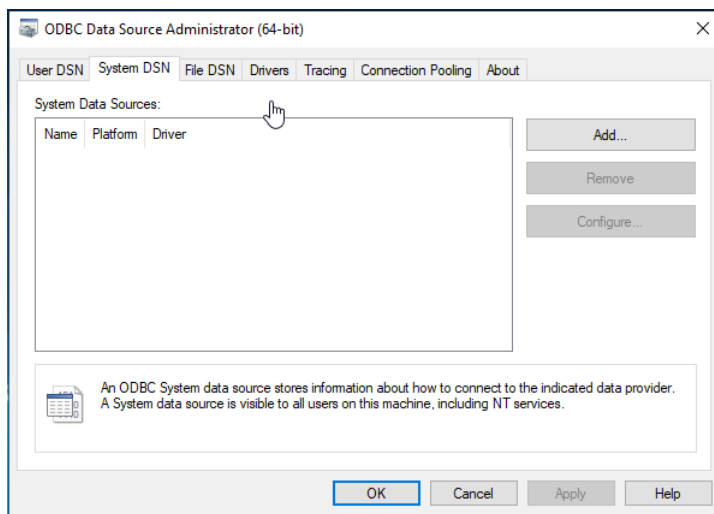
To use a DSN-less connection with ODBC authentication, refer to [Using a DSN-Less Connection with ODBC Authentication](#).

To establish a system DSN

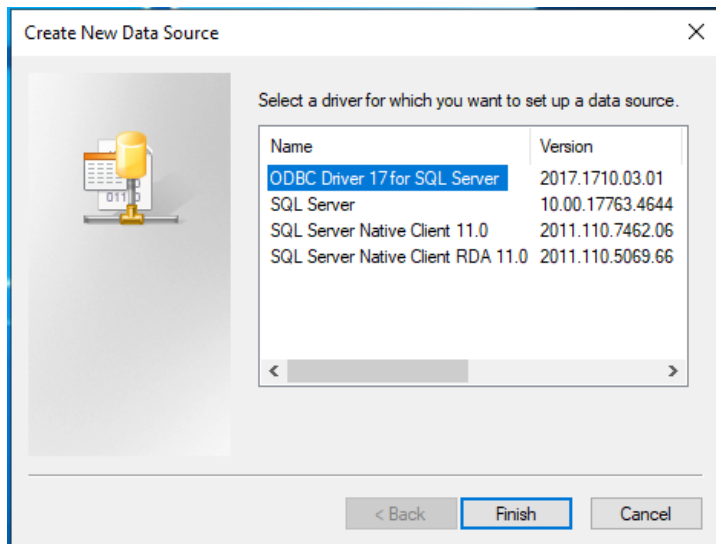
1. In Windows, click **Control Panel, administrative Tools >Data Sources (ODBC)**. The **ODBC Data Source Administrator** appears.



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.

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

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., eftpserver.com)

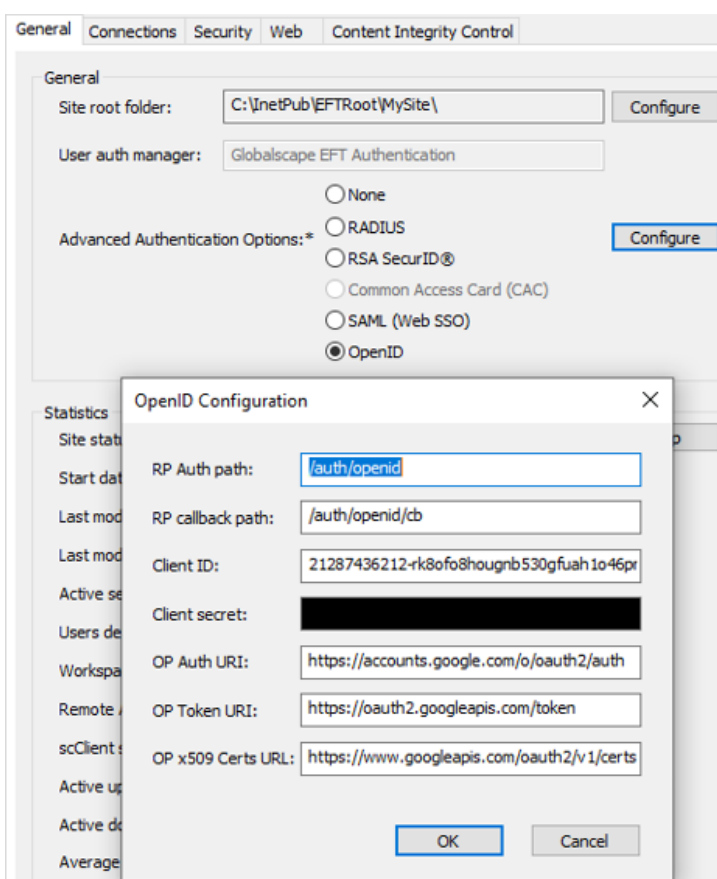
Example of configuring a Google account for OpenID:

1. Set up Google account for 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).

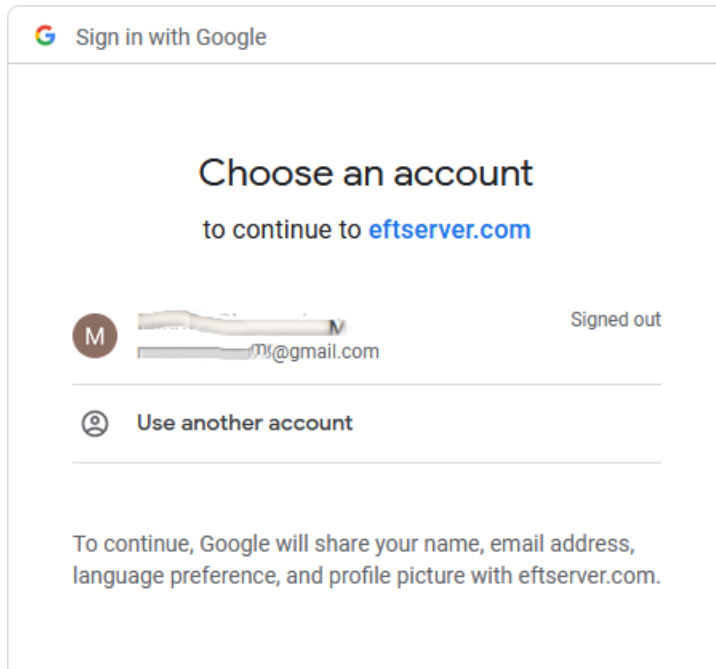
3. Add to the hosts file (C:\Windows\System32\drivers\etc\hosts) on the EFT computer the line below:
127.0.0.1 eftserver.com
4. Restart Windows.
5. In the EFT administration interface on the **Site > Connections** tab, select the **HTTPS** check box and set the **Domain** field to eftserver.com.



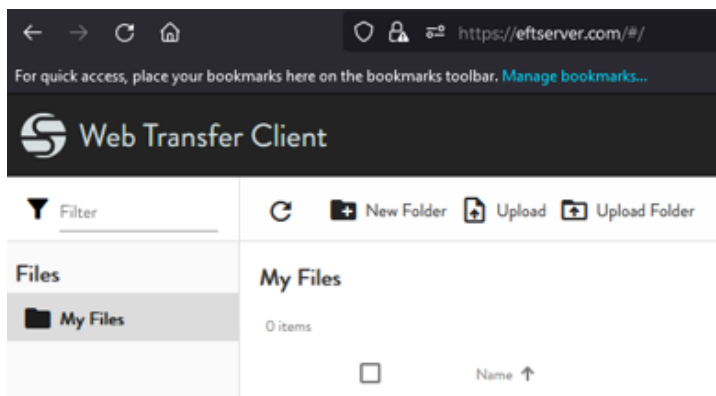
6. On the **Site > General** tab, next to **Advanced Authentication Options**, click **OpenID**, then click **Configure**. The **OpenID Configuration** dialog box appears.



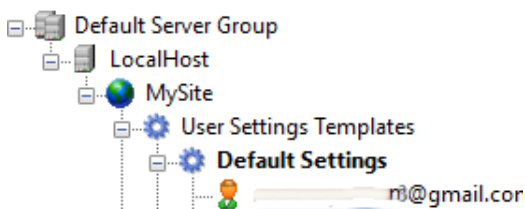
7. Open a browser window and in the browser's address box, type `https://eftserver.com/auth/openid` then press ENTER.



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>.)

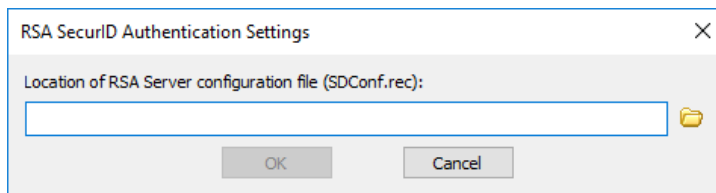
3. The client logs in to the OpenID Provider.
4. The OpenID Provider redirects back to EFT.
The client is added to EFT as a new user and is logged in.

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.

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

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).

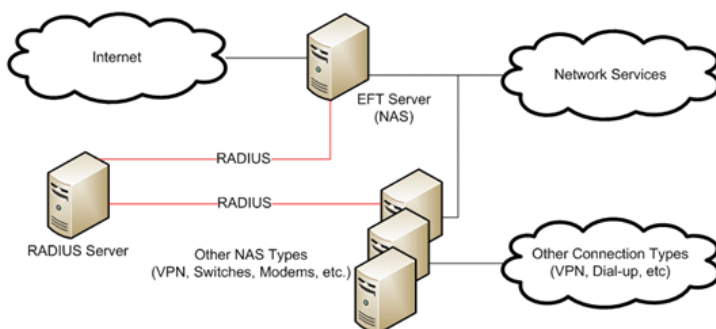
RADIUS and RSA SecurID cannot run together on the same Site. EFT does not support password reset and aging policies for RADIUS or RSA-enabled Sites.

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.

The screenshot shows the 'General' tab of a configuration window. At the top, there are three tabs: 'General', 'Connections', and 'Security'. The 'General' tab is active. Below the tabs, there is a section titled 'General' with several options:

- ☒ Settings Template enabled
 - Status: This is the default Settings Template (ST)
- Description: User Settings Template that provides typical options to n
- ☐ Template root: /
 - The template root folder is only used if a user's Home Folder has been set to "inherit"
- ☒ Treat home folder as the user's default root folder
- ☒ Use RADIUS password management (This checkbox is highlighted with a red box in the image)

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.)"

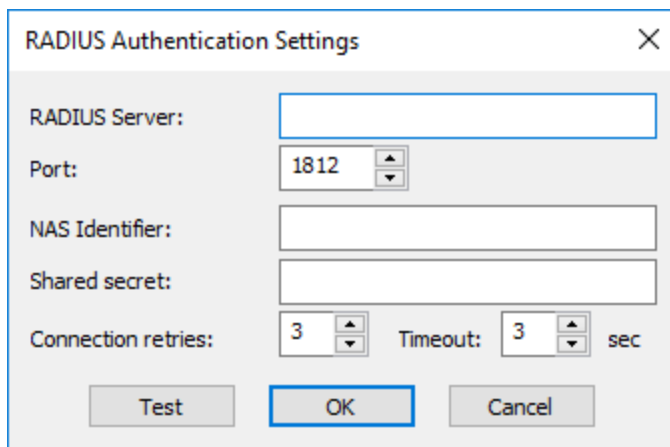
Configuring RADIUS Support on an Existing Site

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.

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

(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:

Reserved Path:

Identity Provider:

Entity ID:

POST URL:

Public Key: 

Username:

Location in assertion: ☐ NameID ☒ Attribute

Attribute name:

Identifier format:

Parse the username using the regular expression:

☒ Extend username lookup to authentication provider

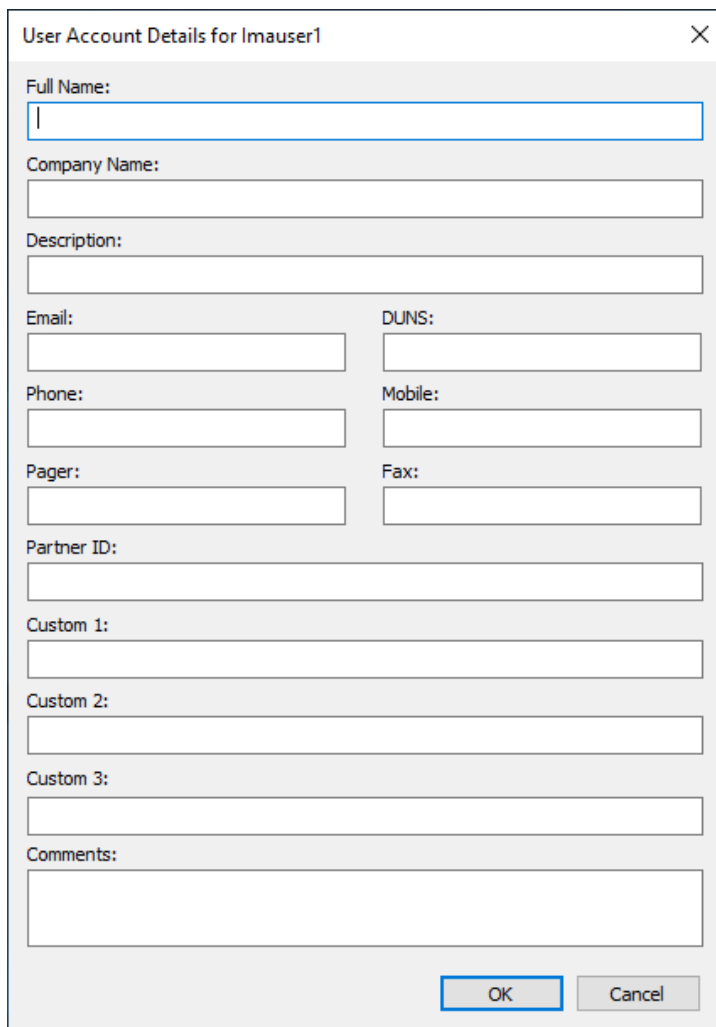
☒ Just in Time (JIT) provisioning (if not found) into:

Email (JIT provisioning):

Location in assertion: ☐ Ignore ☐ Username ☒ Attribute

Attribute Name:

Turn on Trace for SAML logger in logging.cfg



A dialog box titled "User Account Details for lmauser1" with a close button (X) in the top right corner. The dialog contains several input fields for user information:

- Full Name: [text box]
- Company Name: [text box]
- Description: [text box]
- Email: [text box] and DUNS: [text box]
- Phone: [text box] and Mobile: [text box]
- Pager: [text box] and Fax: [text box]
- Partner ID: [text box]
- Custom 1: [text box]
- Custom 2: [text box]
- Custom 3: [text box]
- Comments: [text box]

At the bottom right, there are "OK" and "Cancel" buttons.

- 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.

The screenshot shows the 'General' tab of the EFT Server configuration interface. The 'Site root folder' is set to 'C:\inetpub\eftroot\MySite'. The 'User auth manager' is set to 'Globalscape EFT Authentication'. Under 'Advanced Authentication Options', the 'None' radio button is selected. The 'Statistics' section shows the site is 'Running' with a green status indicator. Other statistics include start date, last modified time, active sessions, users defined, and license information.

General	
Site root folder:	C:\inetpub\eftroot\MySite
User auth manager:	Globalscape EFT Authentication
Advanced Authentication Options:*	☒ None ☐ RADIUS ☐ RSA SecurID® ☐ Common Access Card (CAC) ☐ SAML (Web SSO) ☐ OpenID
Statistics Site status: Running ● Start date/time: Tuesday, October 11, 2022, 14:08:18 Last modified time: Oct 10, 2022. 10:16:34 AM Last modified by: Eftserver1 Active sessions: 0 Users defined: 1 Workspaces licenses: 0 (0 normal, 0 drop-off) assigned / 100 remaining Remote Agent licenses: 1 Licenses Remaining / 1 Total Licenses scClient sessions: 0 active / 0 remaining Active uploads: 0 Active downloads: 0 Average speed: 0 bps	

4. Click **SAML (WebSSO)**, click **Configure**, then provide the details needed to configure SAML.

Web SSO SAML Configuration

Service Provider:

Entity ID:

Reserved Path:

☐ Automatically redirect to the SSO IdP, bypassing the standard login page

Identity Provider:

Entity ID:

POST URL:

Public Key: 

Username:

Location in assertion: ☒ NameID ☐ Attribute

Attribute name:

Identifier format:

Parse the username using the regular expression:

☒ Extend username lookup to authentication provider

☐ Just in Time (JIT) provisioning (if not found) into:

Email (JIT provisioning):

Location in assertion: ☐ Ignore ☒ Username ☐ Attribute

Attribute Name:

Turn on Trace for SAML logger in logging.cfg

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 SAML](#) for 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.

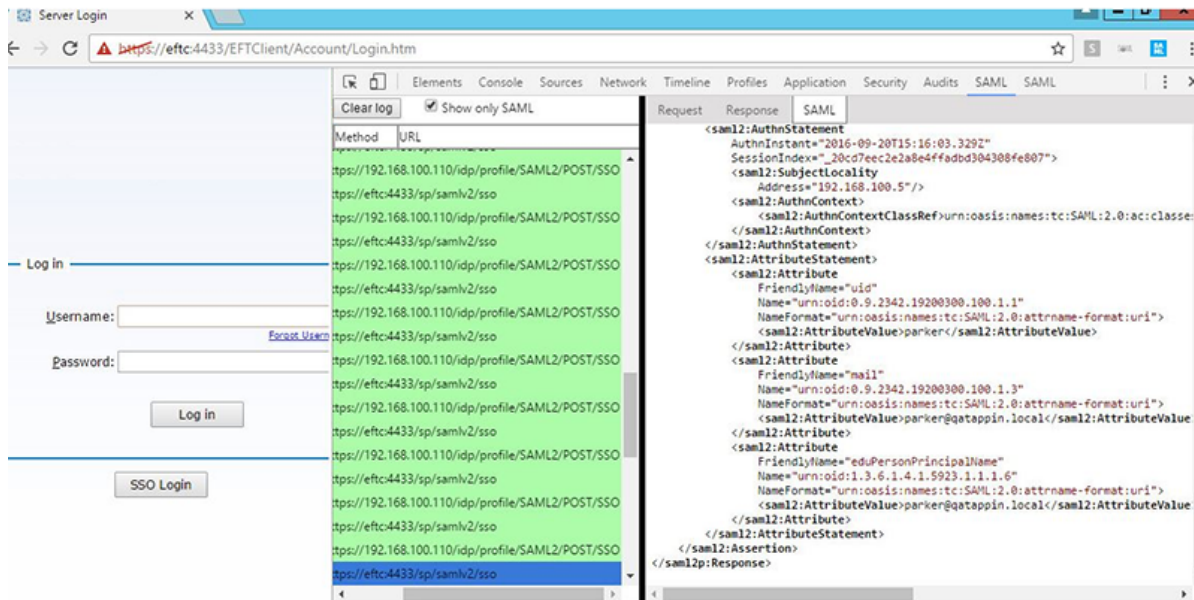
10. EFT will next look up the **user identity** in the claim and attempt to match that username to an existing account in EFT (obtained via directory services called to LDAP, ODBC, or Globalscape authentication provider). If EFT finds an exact match then it knows that the user exists in EFT, where to 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.cfg](#) file, 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 [enabled](#) in 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.php and 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.

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

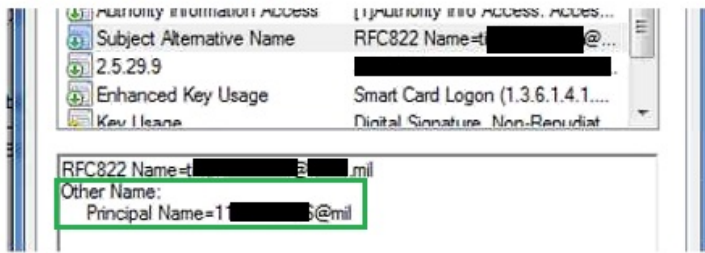
Common Access Card (CAC) Authentication is available for LDAP Sites with SSL (HTTPS or FTPS) enabled. (Requires [Advanced Authentication Modes module](#).)

CAC and Certificates

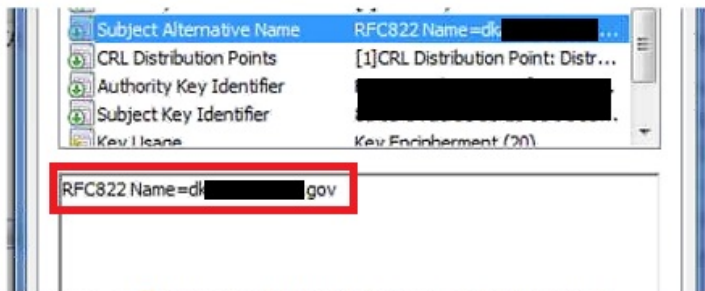
When CAC is enabled on an LDAP Site, clients are required to provide a certificate when connecting. Once the user's certificate is validated, EFT uses the Principal Name (UPN) or RFC822 Name taken from the Subject Alternative Name (SAN) field of the Signature Certificate to search for the user in LDAP 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-authenticated](#) Site.
- 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)

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.

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

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
- 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

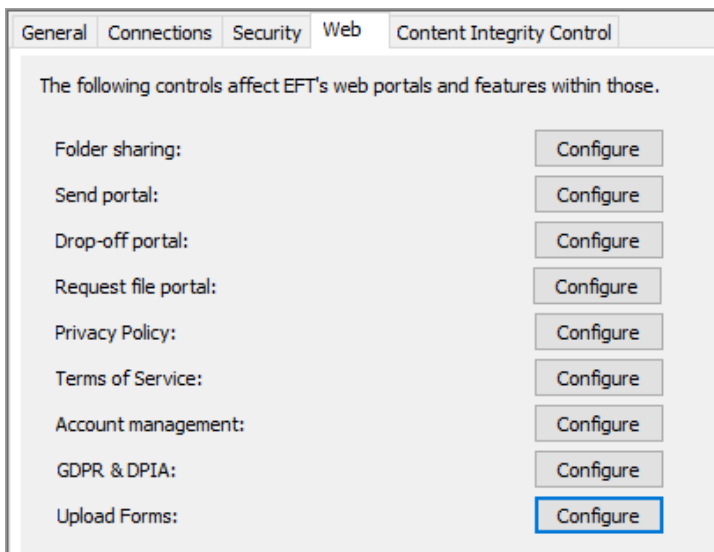
(Requires [Regulatory Compliance Module](#)) The General Data Protection Regulation (GDPR) is a part of European Union (EU) law regarding data protection and privacy in the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's 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 configured [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.

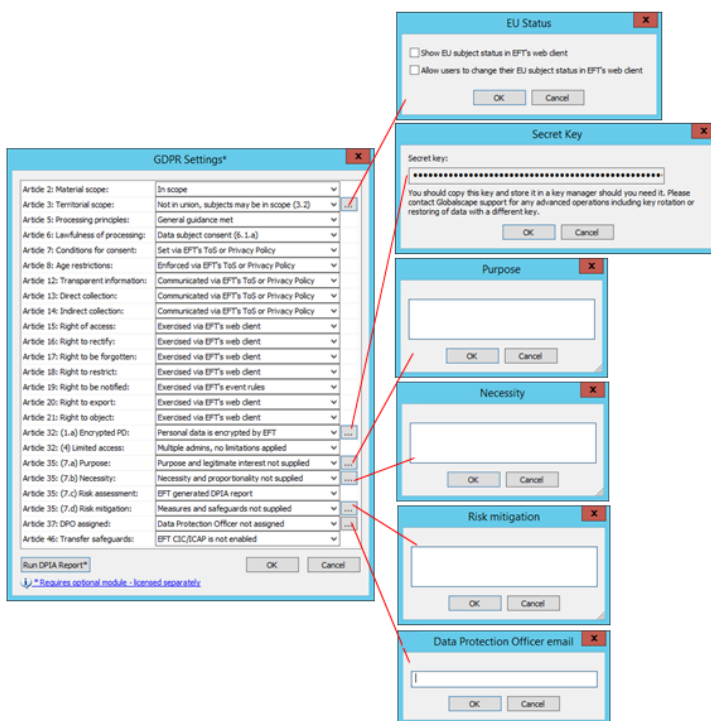


3. Next to GDPR & DPIA, click **Configure**. The **GDPR Settings** dialog box appears.
4. Refer to [Article-by-Article](#) settings below for guidance on how to configure each article.

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)** 0
- **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

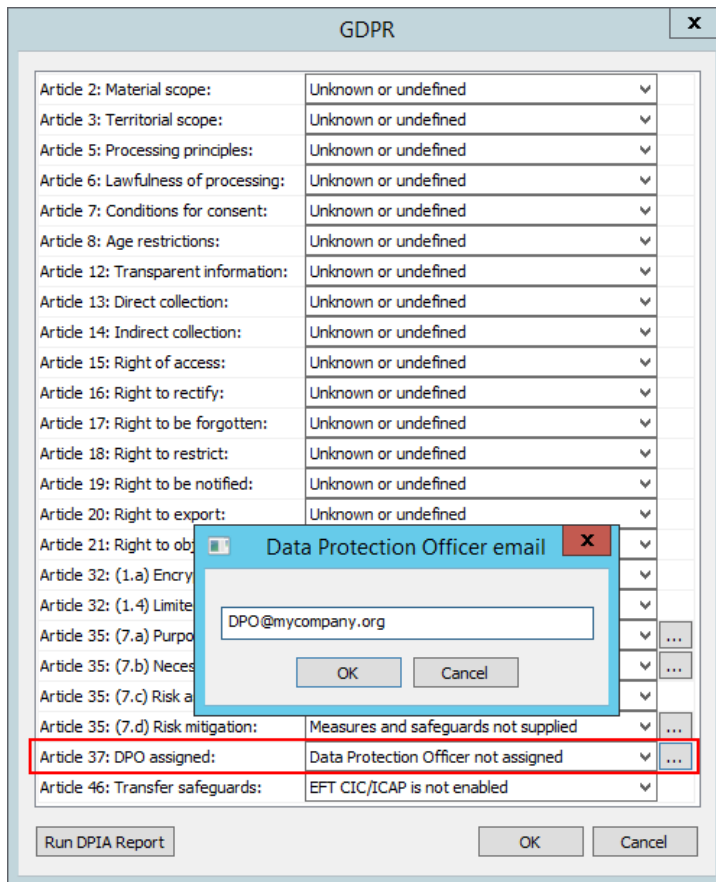
GDPR Data Protection Officer

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 articles](#) that 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**.

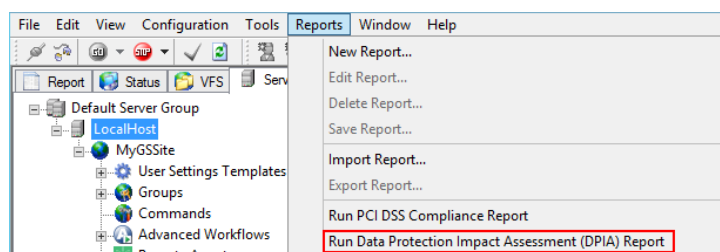


5. Click **OK** to close the **GDPR** dialog box.
6. Click **Apply** on the **Web** tab.

GDPR-DPIA Report

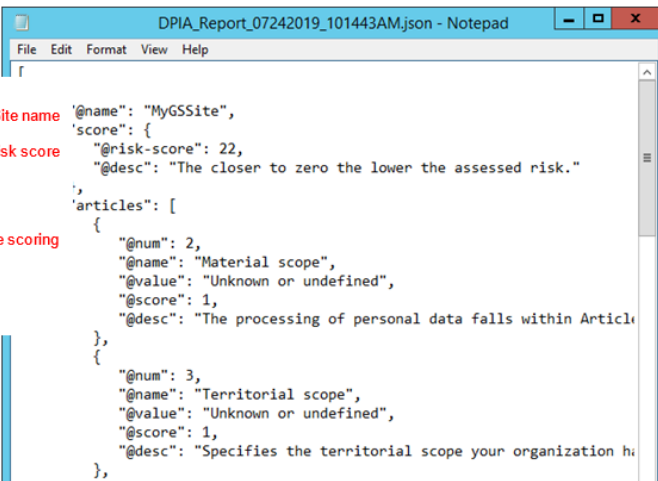
The GDPR Data protection impact assessment (DPIA) helps you identify and minimize the risks to your data. On the Site's [Web](#) tab, when you configure the [GDPR settings](#), you can generate the DPIA report, and a JSON file is created and saved in the EFT installation directory, in the **/Generated 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.)



```

{
  "@name": "MyGSSite",
  "score": {
    "@risk-score": 22,
    "@desc": "The closer to zero the lower the assessed risk."
  },
  "articles": [
    {
      "@num": 2,
      "@name": "Material scope",
      "@value": "Unknown or undefined",
      "@score": 1,
      "@desc": "The processing of personal data falls within Article"
    },
    {
      "@num": 3,
      "@name": "Territorial scope",
      "@value": "Unknown or undefined",
      "@score": 1,
      "@desc": "Specifies the territorial scope your organization h"
    }
  ]
}
```

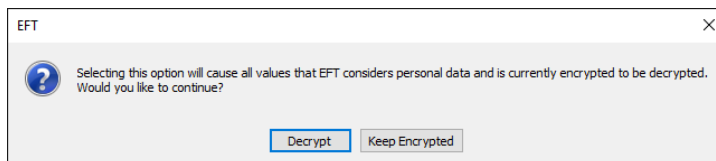
Personal Data Encryption

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.

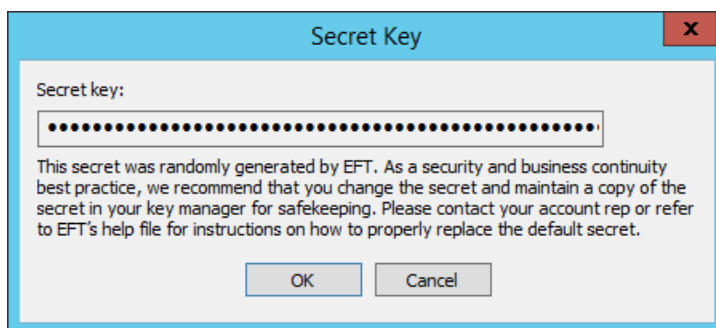
- EFT generates the Personal Data key upon new Site creation.
- Upon upgrade, EFT generates a new key if the Personal Data key is the old "default" value and personal data is not encrypted.
- If your organization has a policy of key rotation every "n" days, you can replace the Personal Data Key manually.

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.

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, FTPS, 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.

Privacy Policy

The Privacy Policy (PP) affects all web-based portals either upon new account registration, anonymous pickup/drop-off if allowed, or after first login.

☒ Enable Privacy Policy (PP)

☐ PP is shown (use for implied consent)

☒ PP consent is required for service (use for GDPR compliance)

☐ Prevent S/FTP/S until PP is agreed to

☒ Revert to implied consent for users identified as not being EU data subjects

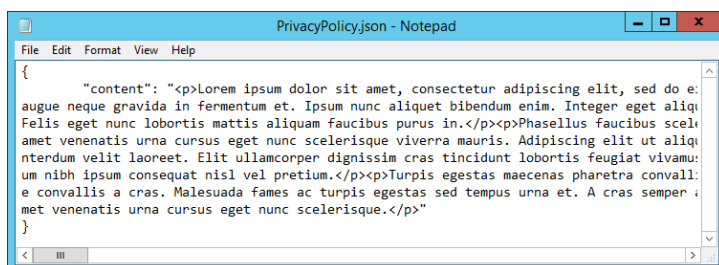
PP agreement(s):

PP agreement labels:

PP agreement effective date: Mar 22, 2019. 01:33:33 PM

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>, , 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

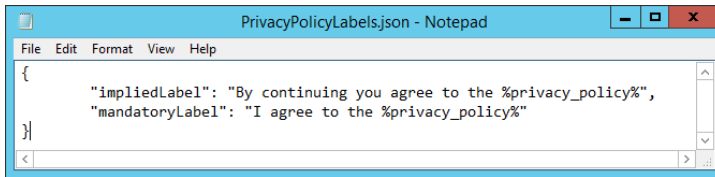
The **PrivacyPolicy** and **PrivacyPolicyLabels** files are JSON files (similar to XML) that must be edited for your organization's agreement. (The labels in the JSON file are case-sensitive.) The files are saved in:

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.

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, FTPS, 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.

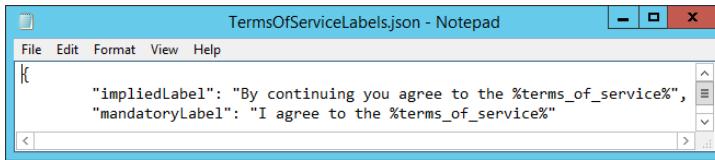
Edit the Terms of Service Agreement and Agreement Labels

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.

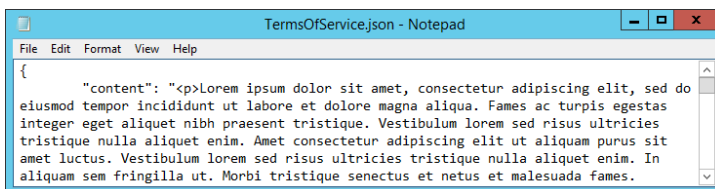
C:\Program Files\Globalscape\EFT Server\Web\Templates\

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 ipsum dolor...") that you will replace with the text of your agreement:



4. Use basic [HTML formatting tags](#) (<p>, , 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.

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.

General

☒ Account enabled ☐ Expire this account on: 3/21/2019

[Change Password](#) Visit the Security tab to change password settings

[Account Details](#) Manage account details templates from Site > Security page

User is EU data subject according to GDPR: Unknown

User consent to Privacy Policy (PP): Unknown

User agreement to Terms of Service (ToS): Unknown

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**.

User Account Details Template

Select a field from the list below to modify its attributes. You can view or modify a unique user's account details on their General page, under Account Details.

Email

Display name: Email

Default value:

Is personal data? ☒

Is modifiable? ☒

Is enabled? ☒

Is visible to user? ☒

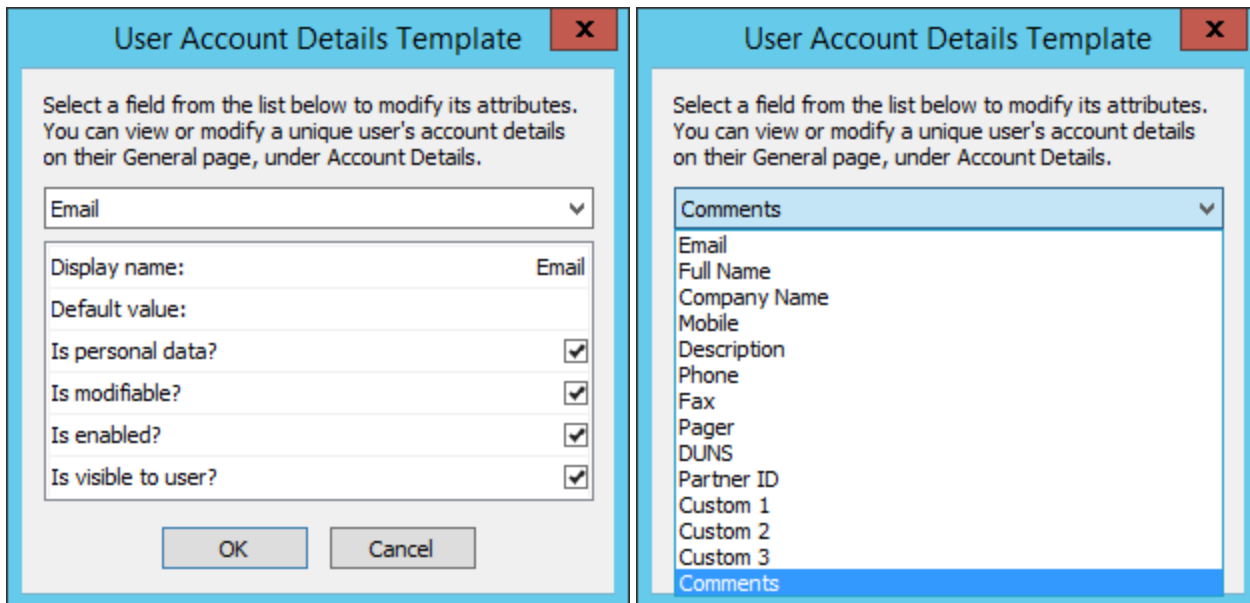
OK Cancel

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.

User Account Details Template

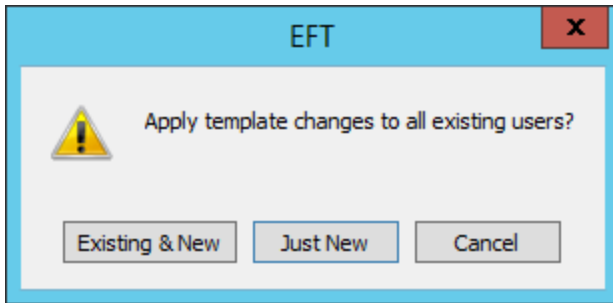
The **User Account Details Template**, available from the **Site > Security** tab, allows you to define which privacy rules will apply to the user account details for **all** user accounts on the Site. Designating attributes to existing account detail fields helps you manage user account details and 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](#).)

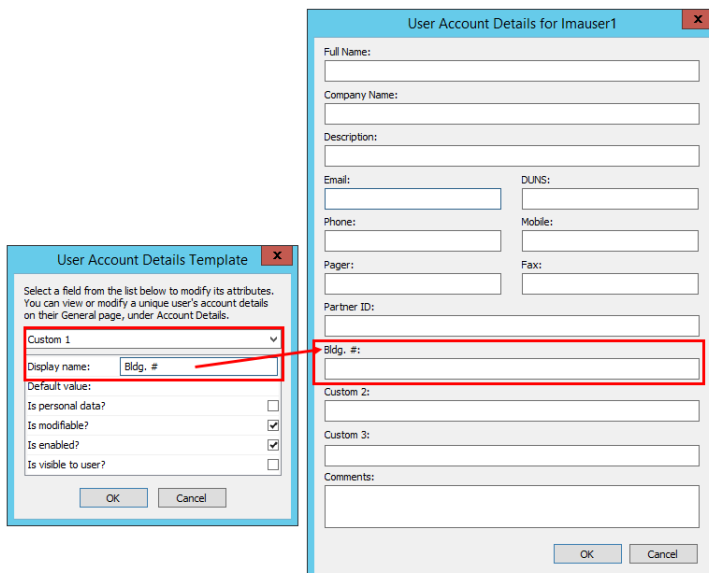


To change the user account fields attributes, default value, and display name

- 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)
- 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	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Is Personal data?	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
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.

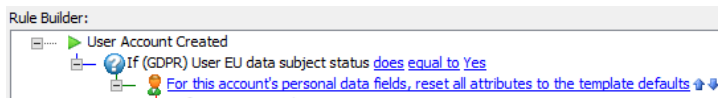
In the example below, the **Pager** field attribute in the User Account Details dialog box is "Visible = true" but the **User Account Details Template** was changed to false (cleared check box). You can leave the setting as-is in the **User Account Details** dialog box, or you can click **Reset All Field Attribute Defaults** to make the field attributes in the **User Account Details** dialog box match the template's settings.

The image shows two side-by-side dialog boxes. The left dialog box is titled "User Account Details for Jsmith17" and contains various input fields for user information. The right dialog box is titled "User Account Details Template" and contains a list of attributes with checkboxes. A red box highlights the "Pager" field in both dialog boxes. In the "User Account Details" dialog, the "Pager" field has a status bar that reads "Personal data = true, Enabled = true, Modifiable = true, Visible = true". In the "User Account Details Template" dialog, the "Pager" field has a status bar that reads "Is personal data? [checked], Is modifiable? [checked], Is enabled? [checked], Is visible to user? [unchecked]". A red arrow points from the status bar in the template dialog to the status bar in the user details dialog.

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.



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. (Updated for PCI DSS v3.2)

Refer to the PCI Security Standards website for [official documentation of the standard](#). You can download the PCI DSS Security Audit Procedures from <https://www.pcisecuritystandards.org>.

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 a Firewall Configuration to Protect Cardholder Data

PCI DSS Requirement	How Requirement is Addressed with EFT
1.1 Establish and implement firewall and router configuration standards.	Requires measures external to EFT.

PCI DSS Requirement		How Requirement is Addressed with EFT
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.		Requires measures external to EFT; however EFT also provides a robust set of IP access filters to control access to EFT and/or the DMZ Gateway.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.		Storing cardholder in the DMZ or other untrusted network is expressly prohibited by PCI DSS (1.3.7). And for security best practices you should not allow inbound connections to originate from untrusted into trusted zones. EFT's optional DMZ Gateway module solves both of these problems. Refer to https://www.globalscape.com/managed-file-transfer/dmz-gateway for details of DMZ Gateway.
	1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	EFT in combination with the DMZ Gateway module facilitates compliance with this requirement.
	1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	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.
	1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.	The need for inbound connections between the DMZ and the internal network is eliminated when using EFT in combination with the DMZ Gateway module.
	1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	Requires measures external to EFT.
	1.3.5 Permit only "established" connections into the network.	EFT can be configured* to use the DMZ Gateway as a SOCKS5 proxy for outbound traffic. Offloading files using EFT though the DMZ Gateway means your internal IP address won't be exposed (1.3.48). Additional steps may be required to fulfill this requirement, such as DLP and deep content inspection tools, before files are submitted to EFT for offloading. *Requires DMZ Gateway.
	1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	EFT, when combined with the DMZ Gateway, eliminates the need to store data in the DMZ.

PCI DSS Requirement		How Requirement is Addressed with EFT
	1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.	Your internal IP addressing scheme is never exposed when EFT is used in combination with the DMZ Gateway.
	1.4 Install personal firewall software on any mobile and/or employee-owned computers	Requires measures external to EFT.
	1.5 Document policies and procedures	Requires measures external to EFT.

Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

PCI DSS Requirement		How Requirement is Addressed with EFT
	2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	When you create a high security-enabled Site, EFT detects 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.
	2.2 Develop configuration standards for all system components.	Refer to the specific sub-requirements below.
	2.2.1 Implement only one primary function per server	EFT's primary function is File Transfer. It is up to the administrator to segregate servers.
	2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	It is up to the administrator to determine whether an enabled protocol is necessary. No protocol is enabled by default.
	2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered insecure.	Any unsecure protocols such as plaintext FTP or HTTP are automatically detected* and you are prompted to change them or present a compensating control.
	2.2.4 Configure system security parameters to prevent misuse.	EFT monitors and warns when • 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

PCI DSS Requirement		How Requirement is Addressed with EFT
	2.2.5 Remove all unnecessary functionality	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.
2.3 Encrypt all non-console administrative access using strong cryptography.		The status of non-console (remote) access settings are monitored and you are warned if SSL is not enabled and given the option to either disable remote administration or enable SSL .
2.4 - 2.6 Inventory maintenance, policy documentation and enforcement, and shared hosting requirements		Requires measures external to EFT.

Requirement 3: Protect Stored Cardholder Data

PCI DSS Requirement		How Requirement is Addressed with EFT
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.		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.
3.2 Do not store sensitive authentication data after authorization (even if encrypted).		3.2.1-3 Refers to card sensitive authentication data (SAD), which should never be stored on the server. Use a third-party DLP or similar tool to detect and prevent SAD storage.
3.3 Mask PAN when displayed		Not applicable to EFT, because EFT cannot display that data.
3.4 Render PAN, at minimum, unreadable anywhere it is stored.		Encrypt PAN or other sensitive data using EFT's optional OpenPGP encryption module or third-party encryption utilities.
	3.4.1 If disk encryption is used, logical access must be managed independently of native operating system authentication and access control mechanisms.	EFT will detect and warn if Microsoft Encrypting File System (EFS) is being used.
3.5 Document and implement procedures to protect keys		Mostly requires measures external to EFT; however access to keys through the administrator interface is limited to administrator roles with Site or Server access only.
3.6 Fully document and implement all key management processes and procedures		Mostly requires measures external to EFT; however, per 3.6.1 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.
3.7 Document policies and procedures		Requires measures external to EFT.

Requirement 4: Encrypt Transmission of Cardholder Data across Open, Public Networks

PCI DSS Requirement	How Requirement is Addressed with EFT
4.1 Use strong cryptography and security protocols	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.
4.2 - 4.3 Never send unprotected PANs by end-user messaging technologies; document security policies and procedures	Requires measures external to EFT.

Requirement 5: Use and Regularly Update Anti-Virus Software

PCI DSS Requirement	How Requirement is Addressed with EFT
5.1 - 5.4 Anti-virus requirements.	Requires measures external to EFT

Requirement 6: Develop and Maintain Secure Systems and Applications

PCI DSS Requirement	How Requirement is Addressed with EFT
6.1 Establish a process to identify security vulnerabilities	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.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	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.
6.3 Develop internal and external software applications securely.	Globalscape takes a number steps to develop secure software, as documented here: https://kb.globalscape.com/KnowledgebaseArticle11061.aspx .
6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	Only applies to Professional Services engagements and should be verified prior to deployment.
6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	Only applies to Professional Services engagements and should be verified prior to deployment.

PCI DSS Requirement	How Requirement is Addressed with EFT
6.4 Follow change control procedures for all changes to system components.	Requires measures external to EFT.
6.5 Address common coding vulnerabilities in software-development processes	Globalscape takes a number steps to develop secure software, as documented here: https://kb.globalscape.com/KnowledgebaseArticle11061.aspx .
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis.	Requires customer to run a security scan. However, Globalscape also performs routine third-party security scans of EFT's public-facing web interfaces as part of its quality assurance process.
6.7 Document policies and procedures	Requires measures external to EFT.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

PCI DSS Requirement	How Requirement is Addressed with EFT
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	EFT provides complete control administrator and user access to resources, with administrator accounts completely segregated from user accounts.
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	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 .
7.3 Document policies and procedures.	Requires measures external to EFT.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

PCI DSS Requirement	How Requirement is Addressed with EFT
8.1 Define and implement policies and procedures to ensure proper user identification management	EFT enforces unique usernames for both users and administrators (8.1.1), provides granular administrative controls over user provisioning and authorization (8.1.2), allows user and administrator account revocation (8.1.3), provides automatic removal of inactive users after 90 days (8.1.4), includes controls for temporarily enabling/disabling users (8.1.5), auto-locks users after six failed login attempts (8.1.6), either for a period of time or permanently until the administrator unbans (8.1.7), and automatically expires sessions after 15 minutes of inactivity (8.1.8)

PCI DSS Requirement	How Requirement is Addressed with EFT
8.2 In addition to assigning a unique ID, ensure proper user authentication.	EFT supports various combinations of password, certificate, two-factor, and public-key authentication mechanisms (8.2), secures passwords during transmission (assumes SSL or SSH), and storage (with a one way [uniquely salted] hash)(8.2.1), verifies identity before allowing password reset or lost username retrieval according to OWASP guidelines (8.2.2), includes minimum length and a number of complexity options (8.2.3), expires and forces password change after 90 days (8.2.4), disallows password re-use, internal dictionary match, or username match (8.2.5), and can force first time use password reset (8.2.6).
8.3 Incorporate two-factor authentication for remote network access. NOTE: EFT does not provide multifactor authentication for remote (non-console) administrator access.	Although EFT supports 2FA, this requirement is about network access, such as what is normally done over a VPN. For compliance with PCI DSS v3.2, you should disable remote (non-console) administrator access. From the PCI DSS v3.2, "Multi-factor authentication is not required at both the system-level and application-level for a particular system component. Multi-factor authentication can be performed either upon authentication to the particular network or to the system component."
8.4 Document and communicate authentication procedures and policies	Requires measures external to EFT.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods	The "Anonymous" password type is disallowed on a high-security-enabled Site. To comply with 8.5.1 you will need to create unique accounts for service provider access, should there ever be a need to provide such access.

PCI DSS Requirement	How Requirement is Addressed with EFT
8.6 Requirements for unique and controlled access using non-standard authentication mechanisms.	Requires measures external to EFT as most of these are physically provisioned to the user.
8.7 All access to any database containing cardholder data is restricted.	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.
8.8 Document policies and procedures.	Requires measures external to EFT

Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS Requirement	How Requirement is Addressed with EFT
9.1 - 9.7 Requirements related to physical access to the cardholder environment.	Requires measures external to EFT.
9.8 Destroy media when it is no longer needed for business or legal reasons. Cardholder data on electronic media must be rendered unrecoverable via a secure wipe program	EFT includes a data-wiping algorithm for sanitizing deleted data on disk.
9.9 Protect devices that capture payment card data via direct physical interaction	Requires measures external to EFT
9.10 Document policies and procedures.	Requires measures external to EFT

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

PCI DSS Requirement	How Requirement is Addressed with EFT
10.1 Implement audit trails to link all access to system components to each individual user	Preconfigured reports of all activity (including administrator actions*) within EFT can be generated on demand with the Auditing and Reporting Module (ARM).
10.2 Implement automated audit trails for all system components	EFT will audit* all user access to data (10.2.1), and all administrator changes** to configuration settings (10.2.2). Access to audit trails, invalid logical access, authentication mechanisms, object creation, and initialization of audit logs (10.2.3-2.7) is managed at the database server.

PCI DSS Requirement	How Requirement is Addressed with EFT
10.3 Record audit trail entries for all system components	EFT audits* user identity (10.3.1), type of transaction (10.3.2), date and time of transaction (10.3.3), transaction result (10.3.4), remote and local IP (10.3.5), and objects affected (10.3.6). *Requires ARM
10.4 Synchronize critical system clocks and times	Requires measures external to EFT.
10.5 Secure audit trails so that they cannot be altered.	Audited data integrity depends on the chosen database solution and authentication architecture. EFT supports auditing to a central SQL or Oracle server.
10.6 Review log and security events for all system components (10.6.1) at least daily	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.
10.7 Retain audit trail history for at least one year	Requires measures external to EFT.
10.8 Implement a process for the timely detection and reporting of failures of critical security control systems	EFT logs and reports audit EFT-specific systems; auditing of other network systems requires measures external to EFT.
10.9 Document policies and procedures	Requires measures external to EFT

Requirement 11: Regularly Test Security Systems and Processes

PCI DSS Requirement	How Requirement is Addressed with EFT
11.1 - 11.6 Requirements relating to regular testing of security systems and processes.	Requires measures external to EFT.

Requirement 12: Maintain a Policy that Addresses Information Security

PCI DSS Requirement	How Requirement is Addressed with EFT
12.1 - 12.10 Maintain a policy that addresses information security for all personnel	Requires measures external to EFT

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

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."

Federal Information Processing Standard (FIPS)

FIPS mode is included in EFT. (Requires SSL/TLS or SFTP modules)

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/FTP (SSL)
 - outbound HTTPs/FTP (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/FTP (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 $\geq$ 2048 bits or ecdsa keys $\geq$ 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 $\leq$ rsa $\leq$ 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 $\geq$ 2048 bits or ecdsa keys $\geq$ 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."

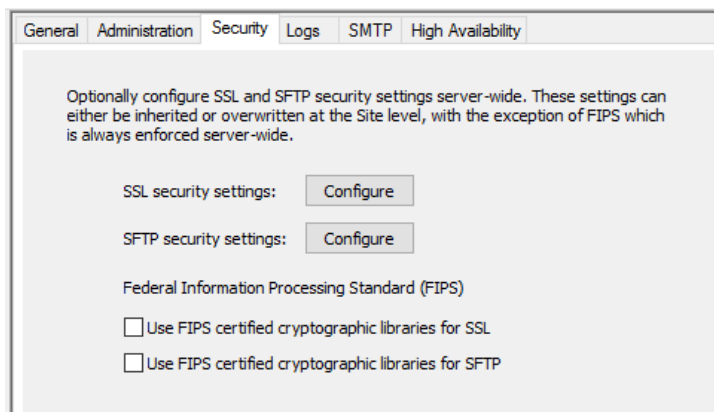
SSL changes	
in nonFIPS mode	Generating rsa keys less than 2048 bit (in GUI only) is prohibited

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.

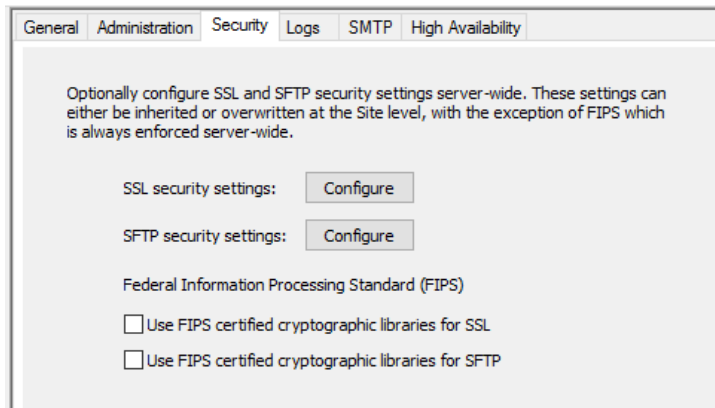
Imported certificates that were signed using non-FIPS-certified algorithms will not work in EFT when using FIPS mode. For details of converting certificates prior to importing them into EFT, refer to [Using OpenSSL to Generate/Convert Keys and Certificates](#).

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.

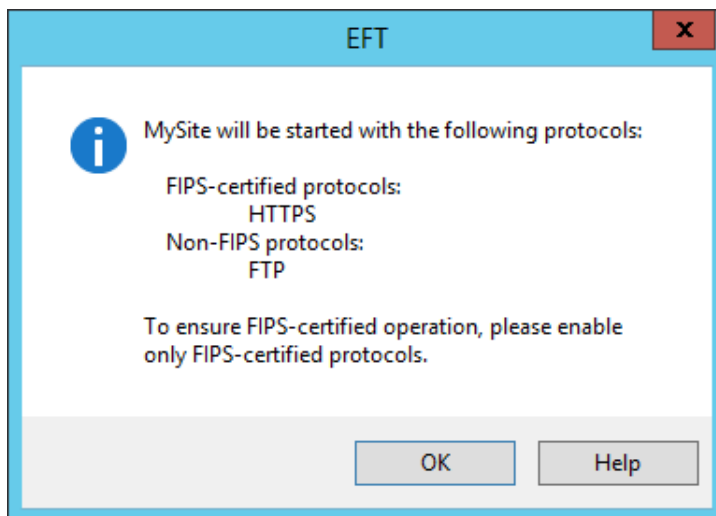
FIPS Mode Event Messages

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

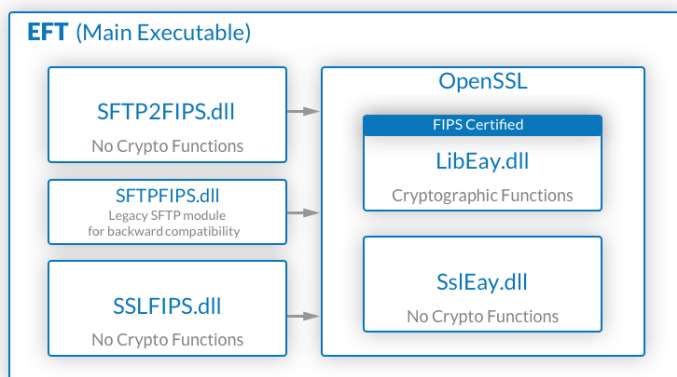
- If you are upgrading from 7.2.9 or 7.3.6 and later to version 7.4.x, and then upgrading to v8.x, you must [export and convert your SFTP keys](#). Version 7.4.x only creates RSA keys in OpenSSH new format. (You can't generate DSS keys and save keys in SSH.com format.)
- After upgrading, the older ciphers 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 [PuTTYGen](#) to 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.

EFT Logging and Visibility

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. Refer to [Log Format, Type, and Location](#) for details of the various logs.

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.

NOTE:

- 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](#).

The EFT client activity (TED6) logs are available as [W3C](#), [Microsoft IIS](#), and [NCSA](#) log file formats. Depending on the log file format selected in administration interface **Server > Logs** tab, a 2-letter abbreviation is prepended to the filename, as described in the table below. The information in the file is the same; it's just in a different file format to accommodate different (external) log readers. Server events are logged to a file named *[log file format]yyymmdd.log*, where YY, MM, and DD indicate the numeric year, month, and day respectively.

For example, a log file in the Microsoft IIS format created on August 22, 2024 is named `in240822.log`.

Log File Format	Abbreviation
W3C	ex
NCSA	nc
Microsoft IIS	in

When using HA, you need to specify a unique location (local) on each node for the log files. This is for troubleshooting purposes (to know on which node an 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.

To specify EFT activity 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](#).

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

EFT Server Log File

The main log for EFT is the **EFT<servername>.log** in the EFT installation folder. (Not affected by the **Server > Logs** tab setting.) If you want to save EFT<servername>.log to a different location, change the reference at the bottom of the **logging.cfg** file to the location [AppDataPath] that you prefer:

```
log4cplus.appender.R.File=${AppDataPath}\EFT.log
```

The EFT <servername>.log files are configured in the **logging.cfg** file in **C:\ProgramData\Globalscape\EFT Server**. Refer to the **logging.cfg** file itself to see which loggers are available to be enabled.

There are 7 log levels: TRACE, DEBUG, INFO, WARN, ERROR, FATAL, and OFF. The levels are hierarchical in nature, so enabling a level enables all levels # to its right (that is, enabling INFO enables WARN, ERROR, and FATAL). Each logger's level can be set independently. Children inherit their parent's level unless explicitly set.

By default the system log level is set to INFO. This will log all INFO, WARN, ERROR, and FATAL log messages. Optionally, you may want to temporarily increase the verbosity of the logging while diagnosing behavior by changing the INFO level to TRACE or DEBUG. Be aware that enabling the TRACE or DEBUG level may have a significant performance impact on the system and may also cause log files to grow rapidly.

```
log4cplus.rootLogger=INFO, RootFileAppender
```

Domain-Level EFT Server Loggers

The logging.cfg file includes a list of more granular loggers. You may optionally enable a custom log level for a particular logger by removing the comment ('#') marker from the beginning of the line. This may be useful when you want to enable more verbose logging for only a particular area of functionality rather than changing the level for the root logger. Be aware that enabling the TRACE or DEBUG level may have a significant performance impact on the system and may also cause log files to grow rapidly. Be sure to comment out the custom log level when you are finished troubleshooting.

SFTP Logging

In the **logging.cfg** file, you can configure logging for SFTP transfers. In the [ARM schema](#), the table **tbl_NegotiatedCiphersSSH** is associated with **tbl_Authentications** and **tbl_Actions**, which tracks the negotiated cipher set for successful SFTP client/server authentications.

- Setting the following [advanced properties](#) to **true** will improve the log performance: **EnableXferLog** (enable transfer logs) and **CloseFinishedItemLog** (false = enabled/default. By default, successful logs are removed.)
- You can see negotiated ciphers in the EFT client log files, for troubleshooting purposes.

To configure logging for SFTP transfers

- Open logging.cfg in a text editor, such as Notepad.
- Find this line:

```
#log4cplus.logger.SFTP=TRACE
```

- Delete the # from the front of the line to enable the logger.
- Leave as TRACE or change to DEBUG for troubleshooting.

If you change it to DEBUG, be sure to change it back to TRACE and/or add the # to the front to comment out (disable) that log to avoid creating unnecessarily large log files.

Note that there are differences in how the logs are displayed depending on whether you are using SFTP.DLL or SFTP2.DLL.

When using the SFTP2.dll, the logs at the KEX section are in ASCII format:

```
08-03-18 07:03:08,947 [3028] INFO Events.Server.MySite.Timer_SFTP_download <Timer: Timer SFTP download: Timer: Timer SFTP download> - Starting Timer for rule
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] id exchange: client protocol version 2.0; client software version clientSftp
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] no match: clientSftp
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] kex: start
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] rekey after 1073741824 bytes, 3600 seconds
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] kex names ok: [diffie-hellman-group16-sha512,diffie-hellman-group14-sha256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1]
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] send packet: type 20
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] SSH2_MSG_KEXINIT sent
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] receive packet: type 20
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] SSH2_MSG_KEXINIT received
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] local server KEXINIT proposal
08-03-18 07:07:16,895 [4852] TRACE SFTP <> - [02A5A8C0] Server key fingerprint 0
```

When using the legacy SFTP.dll, the KEX section is in HEX format:

```

08-03-18 08:15:25,544 [524] TRACE SFTP <> - [02AB4B68] CSftpChannel::CmdStat: /baretail.exe
08-03-18 08:15:25,544 [524] TRACE SFTP <> - [02AB4B68] Sending SSH_MSG_CHANNEL_DATA (42 bytes, seq nr 15)
08-03-18 08:15:25,544 [1964] TRACE SFTP <> - [03AA0FE0] Sending version (hex): 5353482D322E302D312E38325F7373686C696220476C6F62616C73636170650D0A
08-03-18 08:15:25,544 [1964] TRACE SFTP <> - [03AA0FE0] Sending SSH_MSG_KEXINIT (389 bytes, seq nr 0) Data (hex): 142AEC8A2B19E207B881BB200D8D223FF0000007C6469666669652D68656C6C6D616E2D67726F757031362D7368613531322C646966666666
08-03-18 08:15:25,544 [1524] TRACE SFTP <> - [03AA01F8] Sending version (hex): 5353482D322E302D312E38325F7373686C696220476C6F62616C73636170650D0A
08-03-18 08:15:25,544 [1524] TRACE SFTP <> - [03AA01F8] Sending SSH_MSG_KEXINIT (389 bytes, seq nr 0) Data (hex): 141E2BDA89645F634399E454DCF8785EEF0000007C6469666669652D68656C6C6D616E2D67726F757031362D7368613531322C646966666666
08-03-18 08:15:25,544 [1660] TRACE SFTP <> - [03AA07F8] Sending version (hex): 5353482D322E302D312E38325F7373686C696220476C6F62616C73636170650D0A
08-03-18 08:15:25,559 [1524] TRACE SFTP <> - [03AA01F8] Received SSH_MSG_KEXINIT (775 bytes, seq nr 0) Data (hex): 14D6E69FDE638C14B7D561F960600C62000009F6469666669652D68656C6C6D616E2D67726F757031362D7368613531322C646966666666
08-03-18 08:15:25,559 [1524] TRACE SFTP <> - [03AA01F8] Will act on first key exchange method packet
08-03-18 08:15:25,559 [1660] TRACE SFTP <> - [03AA07F8] Sending SSH_MSG_KEXINIT (389 bytes, seq nr 0) Data (hex): 1439420036FFF07D463158F7362AC58B94000007C6469666669652D68656C6C6D616E2D67726F757031362D7368613531322C646966666666
08-03-18 08:15:25,559 [1964] TRACE SFTP <> - [03AA0FE0] Received SSH_MSG_KEXINIT (775 bytes, seq nr 0) Data (hex): 142699563485E80DCD02B34F4525D7D058000009F6469666669652D68656C6C6D616E2D67726F757031362D7368613531322C646966666666
08-03-18 08:15:25,559 [1660] TRACE SFTP <> - [03AA07F8] Received SSH_MSG_KEXINIT (775 bytes, seq nr 0) Data (hex): 14AF17DE0B95880FE99F2EE2B92A44D5A0000009F6469666669652D68656C6C6D616E2D67726F757031362D7368613531322C646966666666
08-03-18 08:15:25,559 [1524] TRACE SFTP <> - [03AA01F8] Will act on first key exchange method packet
08-03-18 08:15:25,622 [1524] TRACE SFTP <> - [03AA07F8] Received SSH_MSG_KEX_30 (517 bytes, seq nr 1)
08-03-18 08:15:25,622 [524] TRACE SFTP <> - [02AB4B68] Received SSH_MSG_CHANNEL_DATA (43 bytes, seq nr 15)

```

SSL/TLS Logging

You can enable to SSL logging to track the details of successful SSL connections. In the [ARM schema](#), the table **tbl_NegotiatedCiphersSSL** is associated with **tbl_Authentications** and **tbl_Actions**, which tracks the negotiated cipher set for successful SSL/TLS client/server authentications.

To track the details of successful SSL connections.

1. Open the logging.cfg file in a text editor such as Notepad.
2. Remove the comment next to #log4cplus.logger.SSL=TRACE, and change TRACE to DEBUG.
3. Remove the comment next to #log4cplus.logger.IPAccess=TRACE.

Example logs:

```

04-10-17 10:16:09,117 [16424] DEBUG IPAccess <>
- Check IP address against IP Access Rules: IP: 127.0.0.1, access
allowed

```

```

04-10-17 10:16:09,117 [7444] DEBUG SSL <> - SSL
connection accepted; protocol version = TLSv1.2, cipher = ECDHE-RSA-
AES128-GCM-SHA256,
key length = 128

```

However, this adds more verbosity to the logs. Additionally, this does not track failed connections and puts the onus on the customer/administrator to pick apart the logs.

For failed connections made via SSL/TLS, the log entry should contain the following:

```

INFO SSL <> - SSL connection failed; ip address=
; connection ID=

```

For successful connections made using insecure ciphers via SSL/TLS, the log entry should contain the following:

```

WARN SSL <> - Insecure SSL connection accepted;
protocol version=; cipher=; key length=; ip address=; connection ID=

```

For successful connections made using weak ciphers via SSL/TLS, the log entry should contain the following:

```
WARN SSL <> - Weak SSL connection accepted; protocol
version=; cipher=; key length=; ip address=; connection ID=
```

SysLogAppender

You can add the SysLogAppender to EFT's logging.cfg file, found in **..\ProgramData\Globalscape\EFT Server** (to send logging information to a security information and event management (SIEM) server, for example).

Add the following code snippet to the bottom of the file. Add comments to inform future users of its purpose.

```
log4cplus.rootLogger=TRACE, syslog
log4cplus.appender.syslog=log4cplus::SysLogAppender
log4cplus.appender.syslog.ident=syslog
log4cplus.appender.syslog.layout=log4cplus::PatternLayout log4cplus.appender.syslog.layout.
ConversionPattern=[%T] %-5p %b %x - %m%n
log4cplus.appender.syslog.host=fdc
log4cplus.appender.syslog.udp=true
log4cplus.appender.syslog.port=514
log4cplus.appender.syslog.facility=user
```

- Refer to <https://kb.globalscape.com/KnowledgebaseArticle11033.aspx> for details of configuring an advanced property to log all HTTP request headers.

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.

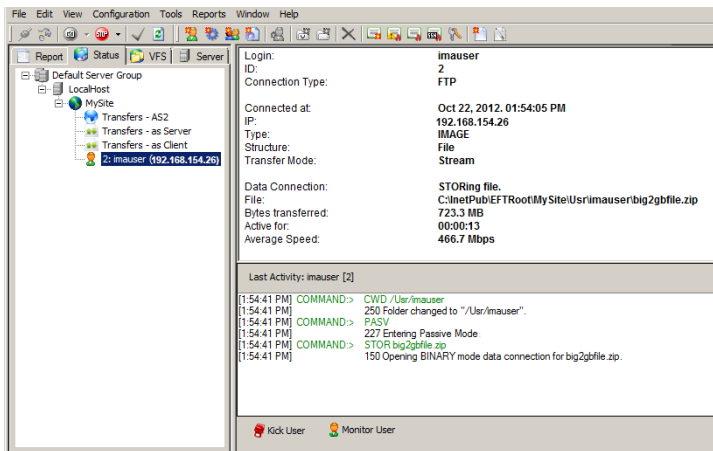
Viewing Connections to a Site

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.

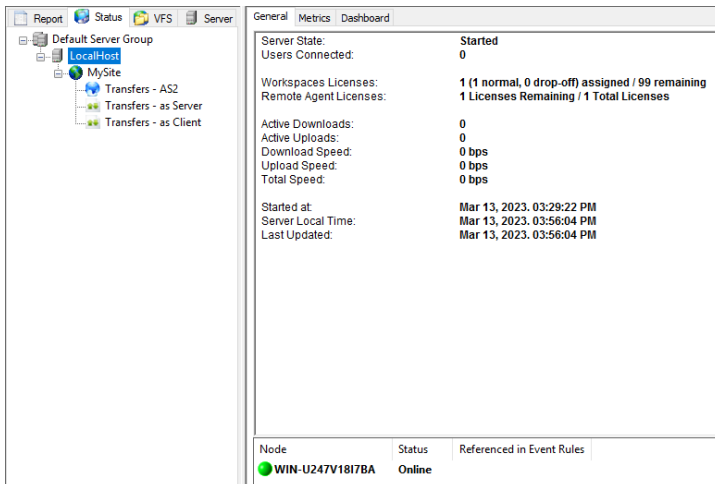


Viewing Server or Node Status

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 Status tab

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 screenshot displays the 'General' tab of the EFT administration interface. The 'General' section contains the following fields and options:

- Site root folder:** C:\inetpub\eftroot\mysite (with a 'Configure' button)
- User auth manager:** Globalscape EFT Authentication
- Advanced Authentication Options:**
 - ☒ None
 - ☐ RADIUS
 - ☐ RSA SecurID®
 - ☐ Common Access Card (CAC)
 - ☐ SAML (Web SSO)
 - ☐ OpenID

The 'Statistics' section provides the following information:

- Site status:** Running (indicated by a green dot) (with a 'Stop' button)
- Start date/time:** Tuesday, October 11, 2022, 14:08:18
- Last modified time:** Oct 10, 2022, 10:16:34 AM
- Last modified by:** Eftserver1
- Active sessions:** 0
- Users defined:** 1
- Workspaces licenses:** 0 (0 normal, 0 drop-off) assigned / 100 remaining
- Remote Agent licenses:** 1 Licenses Remaining / 1 Total Licenses
- scClient sessions:** 0 active / 0 remaining
- Active uploads:** 0
- Active downloads:** 0
- Average speed:** 0 bps

The Site's information appears in the **Statistics** area.

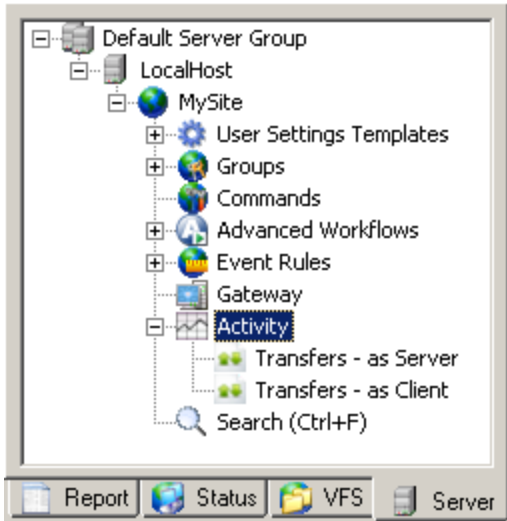
- **Site status:** Displays "Running" or "Stopped"; you can also [stop and start](#) the Site.
- **Start date/time:** Displays the date and time that the Site was last started.
- **Last modified time:** Displays the date and time that the Site was last modified.
- **Last modified by:** Displays the username 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.

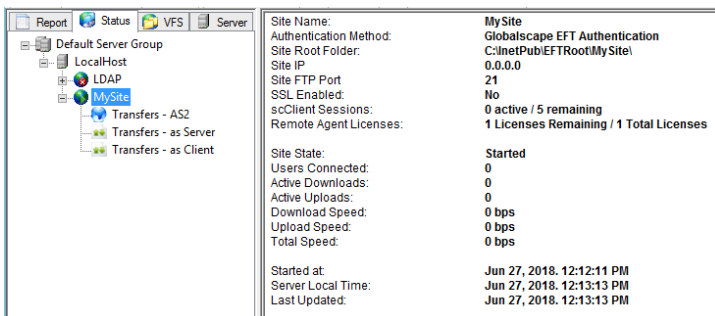
You can view details of transfers to and from EFT on the **Status** tab. Refer to [Viewing Transfers To and From a Site](#) for details.

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.

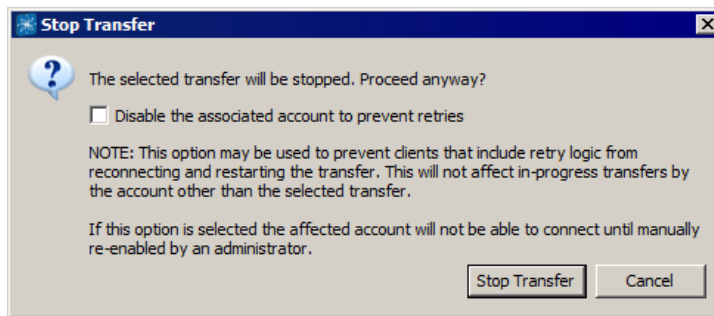
Date/Time	Status	Direction	Username	File Name	Remote...	Protocol	Path	Tran...	Rate	Elapsed
06/29/09-31:56 AM	Success	Receiving	jmbob	win10...	127.0.0.1	HTTPS	C:\D... \Vlen folder	92 B	736 bps	00:00:00
06/29/09-31:56 AM	Success	Receiving	jmbob	_defaut...	127.0.0.1	HTTPS	C:\D... \Vlen folder	707 B	6 bps	00:00:00
06/29/09-31:56 AM	Success	Receiving	jmbob	win102.exe	127.0.0.1	HTTPS	C:\D... \Vlen folder	9 KB	74 bps	00:00:00
06/29/09-31:56 AM	Success	Receiving	jmbob	win10.exe	127.0.0.1	HTTPS	C:\D... \Vlen folder	250 KB	2.0 Mbps	00:00:00
06/29/09-31:55 AM	Success	Receiving	jmbob	WindowsUpdate.log	127.0.0.1	HTTPS	C:\D... \Vlen folder	1.2 MB	10.0 Mbps	00:00:00
06/29/09-29:18 AM	Success	Receiving	jmbob	bootstat.dat	127.0.0.1	HTTPS	C:\D... \Vlen folder	66 KB	541 bps	00:00:00
06/29/09-29:17 AM	Success	Receiving	jmbob	360.exe	127.0.0.1	HTTPS	C:\D... \Vlen folder	58 KB	472 bps	00:00:00
06/29/09-29:17 AM	Success	Receiving	jmbob	Dtdinstall.log	127.0.0.1	HTTPS	C:\D... \Vlen folder	2 KB	14 bps	00:00:00
06/29/09-29:16 AM	Success	Receiving	jmbob	explorer.exe	127.0.0.1	HTTPS	C:\D... \Vlen folder	2.8 MB	13.4 Mbps	00:00:00
06/29/09-29:16 AM	Success	Receiving	jmbob	Freeupdate.exe	127.0.0.1	HTTPS	C:\D... \Vlen folder	13 KB	106 bps	00:00:00
06/29/09-29:15 AM	Success	Receiving	jmbob	msiPName.exe	127.0.0.1	HTTPS	C:\D... \Vlen folder	487 KB	4.0 Mbps	00:00:00
06/29/09-29:14 AM	Success	Receiving	jmbob	Vi.exe	127.0.0.1	HTTPS	C:\D... \Vlen folder	15 KB	119 bps	00:00:00
06/29/09-29:13 AM	Success	Receiving	jmbob	esl_main.log	127.0.0.1	HTTPS	C:\D... \Vlen folder	2 KB	17 bps	00:00:00
06/29/09-29:13 AM	Success	Receiving	jmbob	ESL_main.log	127.0.0.1	HTTPS	C:\D... \Vlen folder	4 KB	24 bps	00:00:00
06/29/09-29:13 AM	Success	Receiving	jmbob	is7.log	127.0.0.1	HTTPS	C:\D... \Vlen folder	74 KB	608 bps	00:00:00
06/29/09-29:12 AM	Success	Receiving	jmbob	mba.bin	127.0.0.1	HTTPS	C:\D... \Vlen folder	42 KB	345 bps	00:00:00
06/29/09-29:11 AM	Success	Receiving	jmbob	msiPName.exe	127.0.0.1	HTTPS	C:\D... \Vlen folder	1 KB	11 bps	00:00:00
06/29/09-29:11 AM	Success	Receiving	jmbob	ocsetup_ocu_install_jfied	127.0.0.1	HTTPS	C:\D... \Vlen folder	32 KB	262 bps	00:00:00
06/29/09-29:10 AM	Success	Receiving	jmbob	nanop.dat	127.0.0.1	HTTPS	C:\D... \Vlen folder	0 B	0 bps	00:00:00

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.

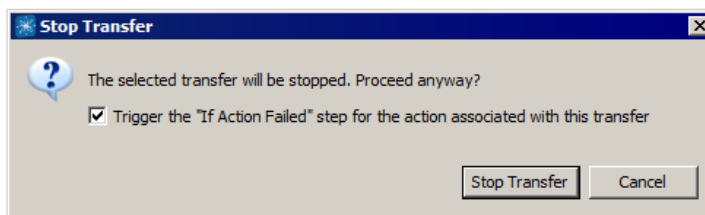
You can:

- 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
Local Port	Server's port on which the file is transferred	x	n/a
Remote Port	Port of remote computer used for transfer	n/a	x
Protocol	Protocol over which the file is transferred	x	x
Path	Path on EFT to which file is transferred	x	n/a
Remote Path	Remote path of file being transferred	n/a	x

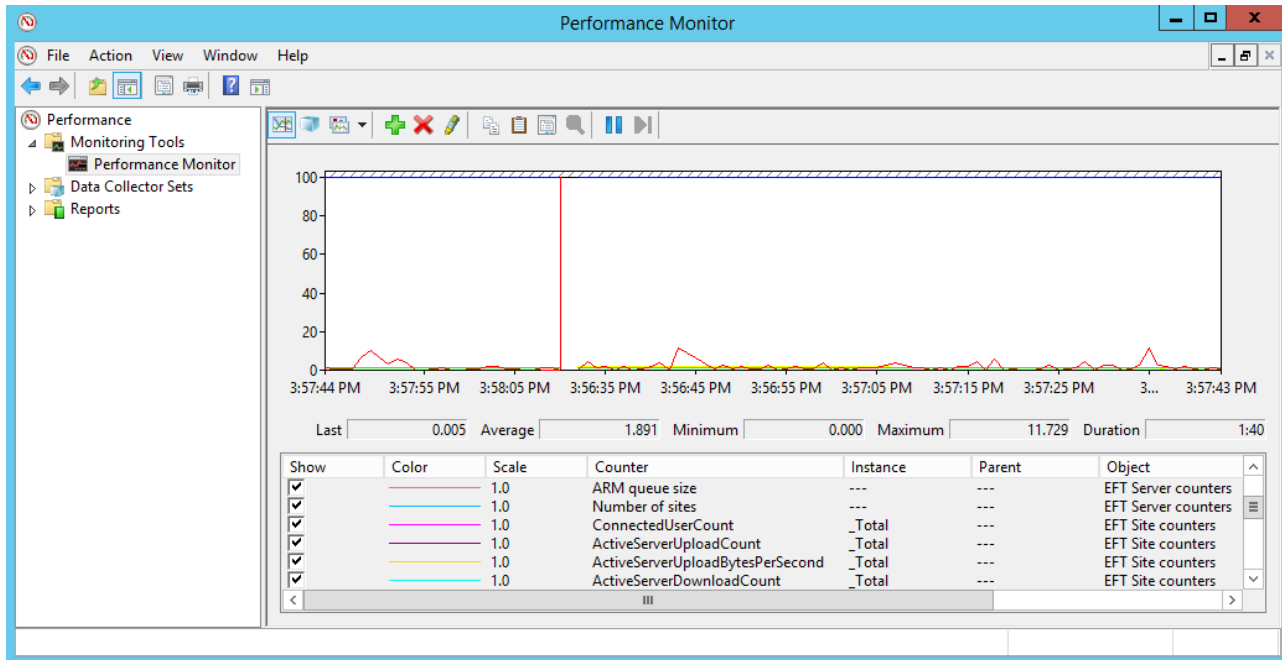
Column	Description	Transfers as Server	Transfers as Client																																		
Local Path	Local path of file being transferred	n/a	x																																		
Transferred	Size of file being transferred	x	x																																		
% Complete	Percentage of transfer completed; 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>	Protocol	EFT as server		EFT as client (that is, Event Rules)		Inbound (client push to server)	Outbound (client pull from server)	Outbound (EFT pushing to client)	Inbound (EFT pulling from client)	HTTP	%	%	%	%	HTTPS	%	%	%	%	FTP	n/a	%	%	%	FTPS	n/a	%	%	%	SFTP	n/a	n/a	%	%	x	x
Protocol	EFT as server		EFT as client (that is, Event Rules)																																		
	Inbound (client push to server)	Outbound (client pull from server)	Outbound (EFT pushing to client)	Inbound (EFT pulling from client)																																	
HTTP	%	%	%	%																																	
HTTPS	%	%	%	%																																	
FTP	n/a	%	%	%																																	
FTPS	n/a	%	%	%																																	
SFTP	n/a	n/a	%	%																																	
Rate	Rate, in kilobits per second (kbps), at which the file is transferred	x	x																																		
Elapsed	Time in HH:MM:SS that it took to transfer the file	x	x																																		

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 ARMLogStalledThreadadministratorDuration (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

Server-Level Counters	Counter	Description
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
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

Site-Level Counters	Counter	Description
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
	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 there 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

Site-Level Counters	Counter	Description
	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.
	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](#).

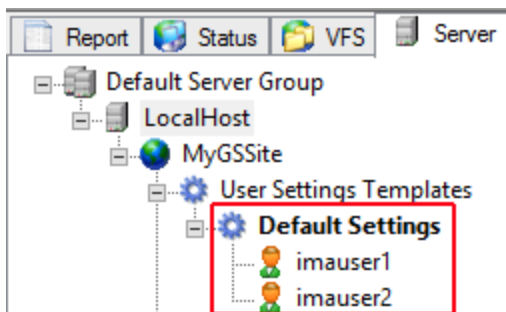
For information about using Performance Monitor, refer to [Windows Performance Monitor Overview](#) on the Microsoft Tech Community website.

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.

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.

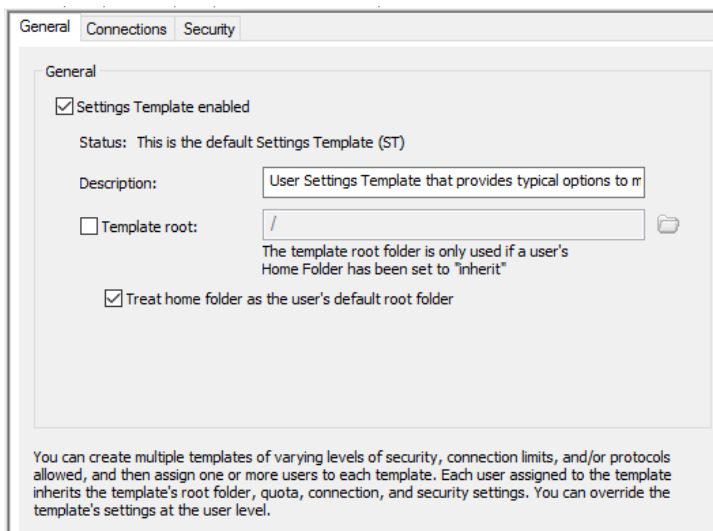
Settings Templates apply to the Server resources. Use [permissions](#) assigned to Groups to control access to folders on your system.

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 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](#).



The screenshot shows the 'General' tab of a Settings Template configuration window. The window has three tabs: 'General', 'Connections', and 'Security'. The 'General' tab is active and contains the following settings:

- ☒ Settings Template enabled
- Status: This is the default Settings Template (ST)
- Description: User Settings Template that provides typical options to n
- ☐ Template root: /
- ☒ Treat home folder as the user's default root folder

Below the settings, there is a note: "The template root folder is only used if a user's Home Folder has been set to 'inherit'". At the bottom of the window, there is a paragraph of text: "You can create multiple templates of varying levels of security, connection limits, and/or protocols allowed, and then assign one or more users to each template. Each user assigned to the template inherits the template's root folder, quota, connection, and security settings. You can override the template's settings at the user level."

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](#).

The screenshot shows the 'Connections' tab of a Settings Template configuration window. The window has three tabs: 'General', 'Connections' (selected), and 'Security'. Below the tabs, there is a section titled 'Specify the settings for users assigned to this template.' which contains two main sections: 'Protocols' and 'Network Usage & Limits'.

Protocols Section:

- ☐ FTP: FTP configuration options: [FTP Config](#)
- ☐ FTPS (SSL/TLS)*: SSL authentication options: [SSL Auth](#)
- ☐ SFTP (SSH2)*: SFTP authentication options: [SFTP Auth](#)
- ☐ HTTP*
- ☒ HTTPS*:
 - ☒ Allow Web Transfer Client (WTC) over HTTP/S
 - ☒ Allow secure folder sharing*
 - ☒ Allow secure file sending (web and Outlook add-in)*
 - ☐ Require additional factor(s) for authentication*
- ☐ AS2 inbound*
- ☐ AS2 outbound*

Network Usage & Limits Section:

- Connection limits: [Configure](#)
- Transfer limits: [Configure](#)
- IP access/ban list: [Configure](#)

At the bottom of the window, there is a blue information icon followed by the text: [* Requires optional module - licensed separately](#)

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.

The screenshot shows the 'Security' tab of a settings template configuration window. It has three sub-tabs: 'General', 'Connections', and 'Security'. The 'Security' tab is active. It is divided into two main sections: 'Password Security' and 'Account Security'.

Password Security:

- Invalid login options:** Includes a 'Configure' button and two settings:
 - ☐ Enforce strong passwords (with a link icon and a 'Configure' button)
 - ☐ Allow users to reset their passwords
 - ☐ Force new users to change their first-time password immediately upon first use
- Password expiration options:** Includes a 'Configure' button and one setting:
 - ☐ Prohibit reuse of previous [dropdown] passwords

Account Security:

- ☐ Disable [dropdown] account after [dropdown] days of inactivity

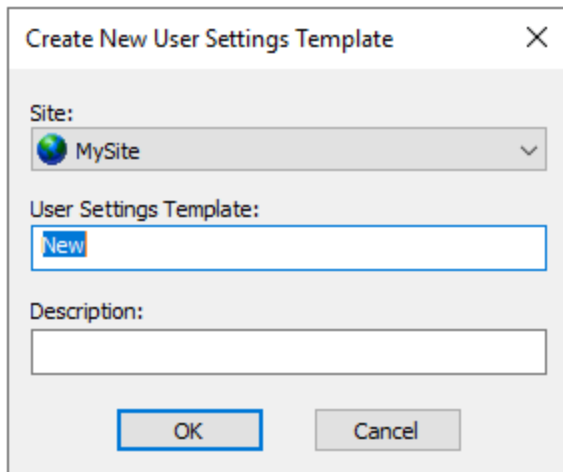
Creating or Deleting Settings Templates

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.



The dialog box is titled "Create New User Settings Template" with a close button (X) in the top right corner. It contains three input fields: "Site:" with a dropdown menu showing "MySite", "User Settings Template:" with a text box containing "New", and "Description:" with an empty text box. At the bottom are "OK" and "Cancel" buttons.

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.

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 .

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.

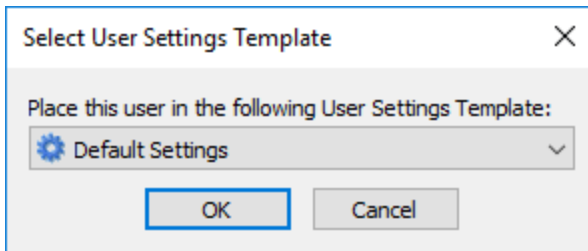
You can move only one user at a time, using drag and drop or the procedure below.

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**.

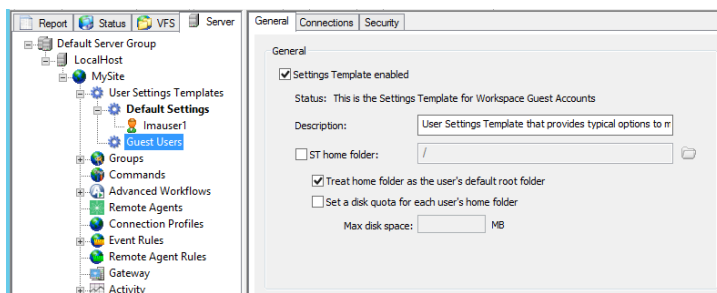
The **Select User Settings Template** dialog box appears.



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 [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](#). 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.

General Connections Security

Specify the settings for users assigned to this template.

Protocols

☐ FTP FTP configuration options: [FTP Config](#)

☐ FTPS (SSL/TLS)* SSL authentication options: [SSL Auth](#)

☐ SFTP (SSH2)* SFTP authentication options: [SFTP Auth](#)

☐ HTTP*

☒ HTTPS*

☒ Allow Web Transfer Client (WTC) over HTTP/S

☒ Allow secure folder sharing*

☒ Allow secure file sending (web and Outlook add-in)*

☐ Require additional factor(s) for authentication*

☐ AS2 inbound*

☐ AS2 outbound*

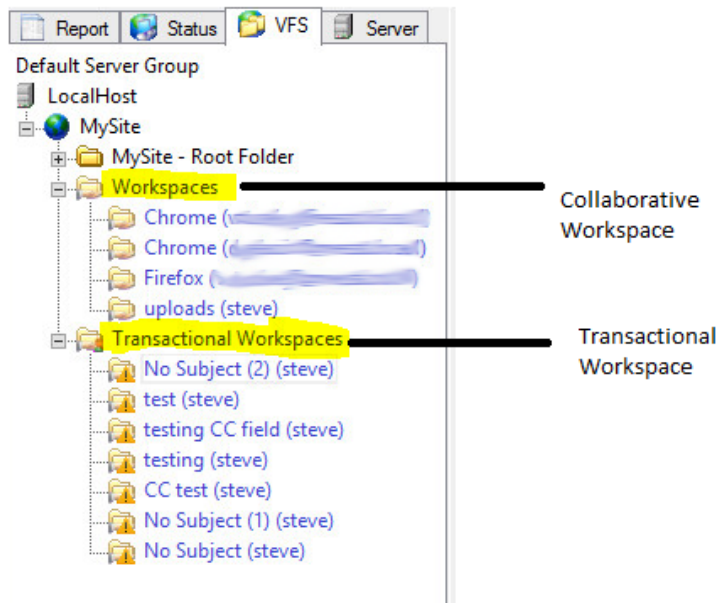
Network Usage & Limits

Connection limits: [Configure](#)

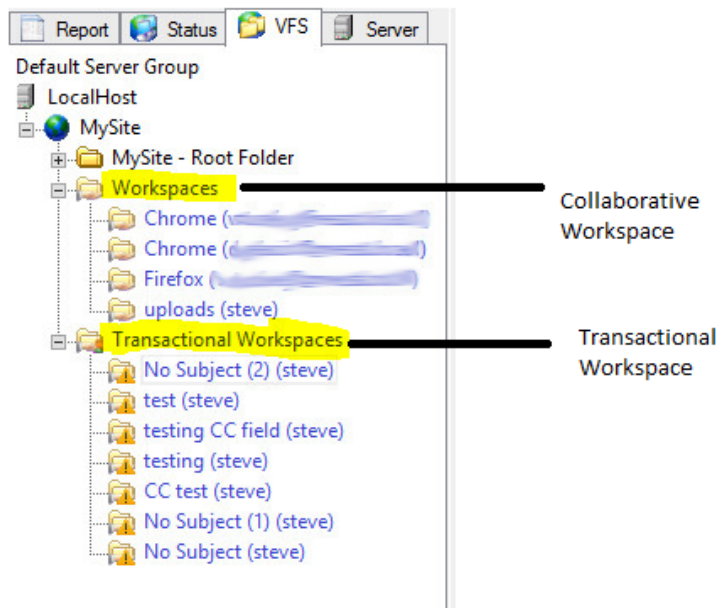
Transfer limits: [Configure](#)

IP access/ban list: [Configure](#)

[* Requires optional module - licensed separately](#)



Guest users' folders are created in the [VFS](#) in the Transactional Workspaces node of the Site.



User Tabs

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](#).

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 Site](#) or 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**.

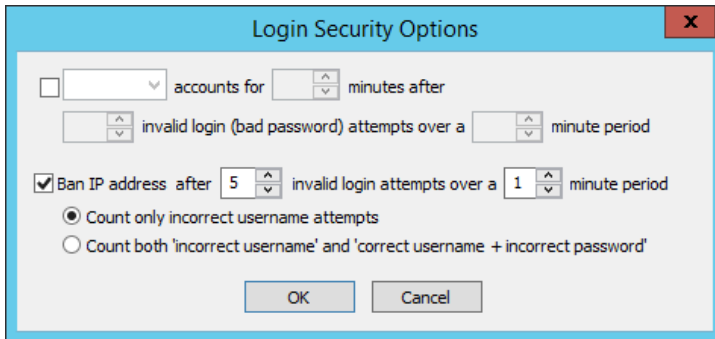
Banning an IP Address that Uses an Invalid Account

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.)

User Tabs

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

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.

The screenshot shows the 'General' tab of a user account configuration window. At the top, there are three tabs: 'General', 'Connections', and 'Security'. The 'General' tab is active.

General

- ☒ Account enabled ☐ Expire this account on: 4/13/2022
- [Change Password](#) Visit the Security tab to change password settings
- [Account Details](#) Manage account details templates from Site > Security page
- User is EU data subject according to GDPR: * Unknown
- User consent to Privacy Policy (PP): Unknown
- User agreement to Terms of Service (ToS): Unknown
- ☒ User home folder: /usr/Imauser1/ 📁
- ☒ Treat home folder as the user's default root folder

Statistics

Status:	Not connected	Kick user
	Not locked	Unlock
Last time connected:	N/A	
Account created:	Apr 13, 2022. 11:16:39 AM	
Last modified by:	Eftserver1	
Last modified time:	Apr 13, 2022. 11:16:39 AM	
Last password change:	Apr 13, 2022. 11:16:39 AM	

[* Requires optional module - licensed separately](#)

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.

The screenshot shows the 'Connections' tab of a user account settings window. The window has three tabs: 'General', 'Connections', and 'Security'. The 'Connections' tab is active. Below the tabs, there is a section titled 'Specify the settings for this user.' followed by a 'Protocols' section. In the 'Protocols' section, there are several options: 'FTP', 'FTPS (SSL/TLS)*', 'SFTP (SSH2)*', 'HTTP*', and 'HTTPS*'. The 'HTTPS*' option is selected with a checkmark. To the right of these options are buttons for 'FTP Config', 'SSL Auth', and 'SFTP Auth'. Below the 'HTTPS*' option, there are three sub-options: 'Allow Web Transfer Client (WTC) over HTTP/S', 'Allow secure folder sharing*', and 'Allow secure file sending (web and Outlook add-in)*', all of which are checked. Below these are 'AS2 inbound*' and 'AS2 outbound*' options, each with a corresponding button ('AS2 Inbound' and 'AS2 Outbound'). At the bottom of the 'Protocols' section is a 'Network Usage & Limits' section with three rows: 'Connection limits:', 'Transfer limits:', and 'IP access/ban list:', each with a 'Configure' button. At the very bottom of the window, there is a blue information icon followed by the text '* Requires optional module - licensed separately'.

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.

The screenshot shows a settings window with three tabs: General, Connections, and Security. The Security tab is active. It contains two main sections: Password Security and Account Security.

Password Security

- Invalid login options: [Configure](#)
- ☐ Enforce strong passwords [Configure](#)
- ☐ Allow users to reset their passwords
 - ☐ Force user to change their password immediately upon next use
- Password expiration options: [Configure](#)
- ☐ Prohibit reuse of previous passwords

Account Security

- ☐ [Disable](#) account after days of inactivity
- Account group membership: [Groups...](#)

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 .)

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.

User Account Details for Imauser1

Full Name:

Company Name:

Description:

Email: kmarsh@globalscape.com DUNS:

Phone: Mobile:

Pager: Fax: Personal data = true, Enabled = true, Modifiable = true, Visible = true

Partner ID:

Custom 1:

Custom 2:

Custom 3:

Comments:

User Account Details Template

Select a field from the list below to modify its attributes. You can view or modify a unique user's account details on their General page, under Account Details.

Mobile

Display name: Mobile

Default value:

Is personal data? ☒

Is modifiable? ☒

Is enabled? ☒

Is visible to user? ☒

OK Cancel

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 [General](#) tab.
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.

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 /U_sr/%USER.LOGIN%.)

4. (Optional) Click **Details**. The **New User Account Details** dialog box appears.

The screenshot shows a dialog box titled "User Account Details for Imauser1". It contains the following fields and labels:

- Full Name: [text box]
- Company Name: [text box]
- Description: [text box]
- Email: [text box]
- DUNS: [text box]
- Phone: [text box]
- Mobile: [text box]
- Pager: [text box]
- Fax: [text box]
- Partner ID: [text box]
- Custom 1: [text box]
- Custom 2: [text box]
- Custom 3: [text box]
- Comments: [text box]

At the bottom right, there are two buttons: "OK" and "Cancel".

- 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.

[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.)

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.

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.

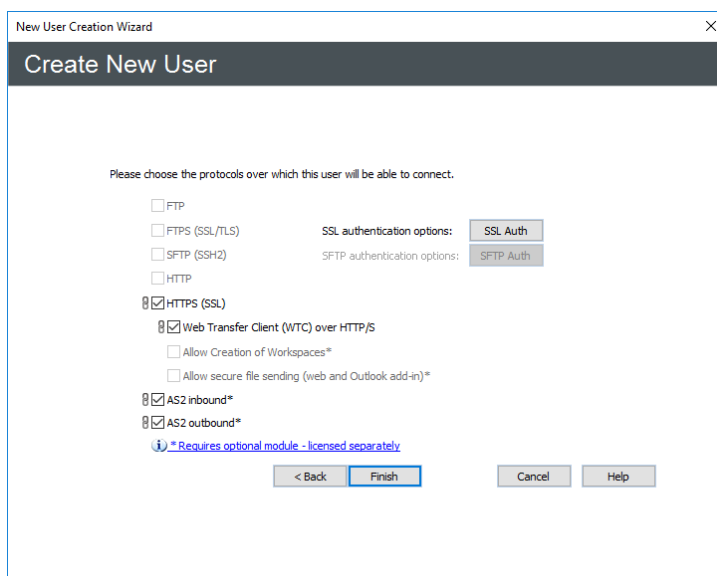
If you use `/usr/` as the account's home folder (and remove the default `%USER.LOGIN%`) and clear the **Grant FULL permissions to user in this folder** check box, the account will inherit the permissions of the `/usr/` folder, which are **Show this folder in parent list** and **Show files and folder 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](#).

- Next to **Assign group membership**, click **Groups**. The **Group Membership** dialog box appears.
- 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**.
- Click **Next**. The protocols page appears.



- 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.

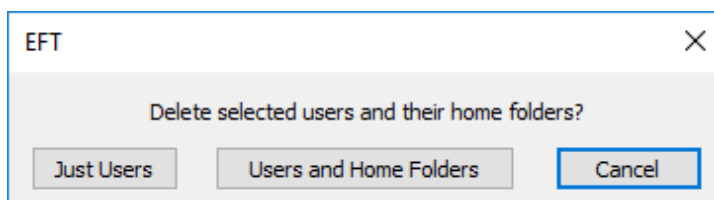
Deleting a User Account

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.

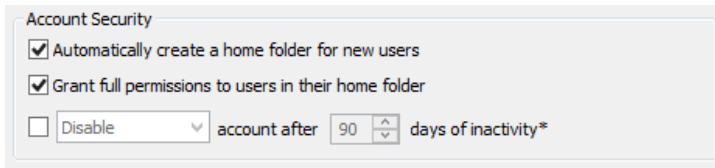
When a high security-enabled Site is created in the Site Setup wizard, the option to delete inactive [user](#) and [administrator accounts](#) after 90 days is enabled by default. If during Site setup EFT detects that one or more administrator accounts already exist, and that the option to delete administrator 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"

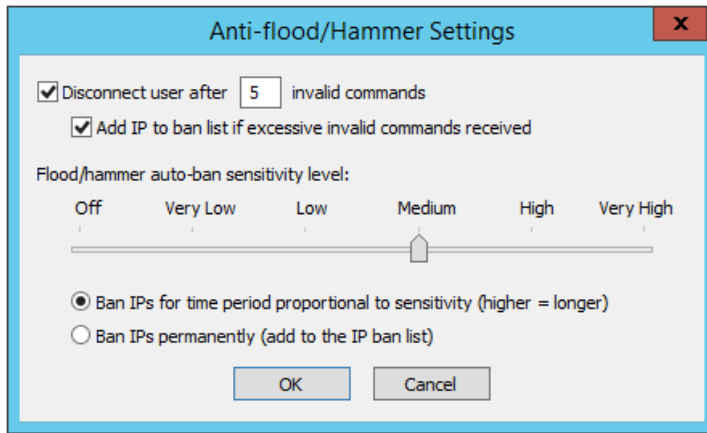
In the message that appears, you can discard the change or accept the non-compliant setting and provide a reason for using this setting (for example, if you are using an alternate solution). If you accept the change and provide a reason, the warning and the reason that you provided appear in the [PCI DSS Compliance report](#).

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](#).

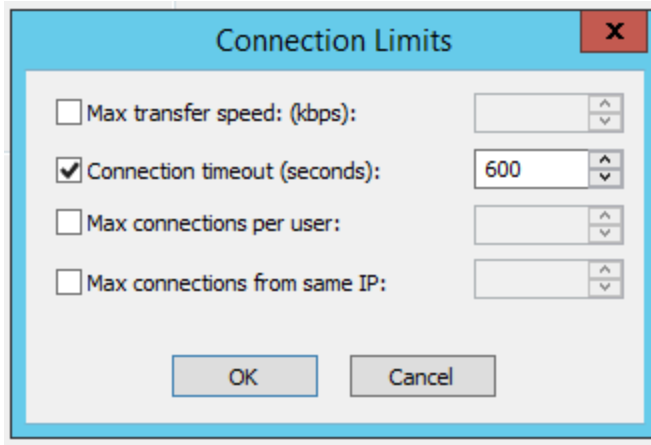
Disconnecting Users on Timeout

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.

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 [General](#) tab.
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 .
 - 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 [General](#) tab.
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

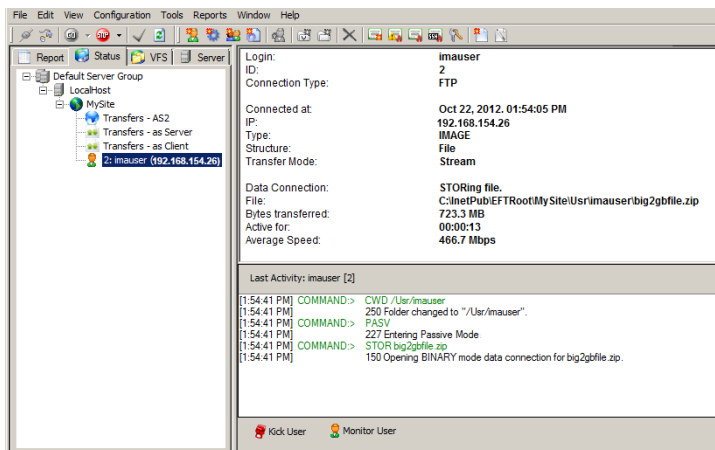
1. In the administration interface, [connect to EFT](#) and click the **Server** tab.
2. On the **Server** tab, click the user account that you want to enable.
3. In the right pane, click the [General](#) tab.
4. Clear the **Expire this account on** check box and select the **Enable this user account** 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 **insensitive**. 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.Quit(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-----

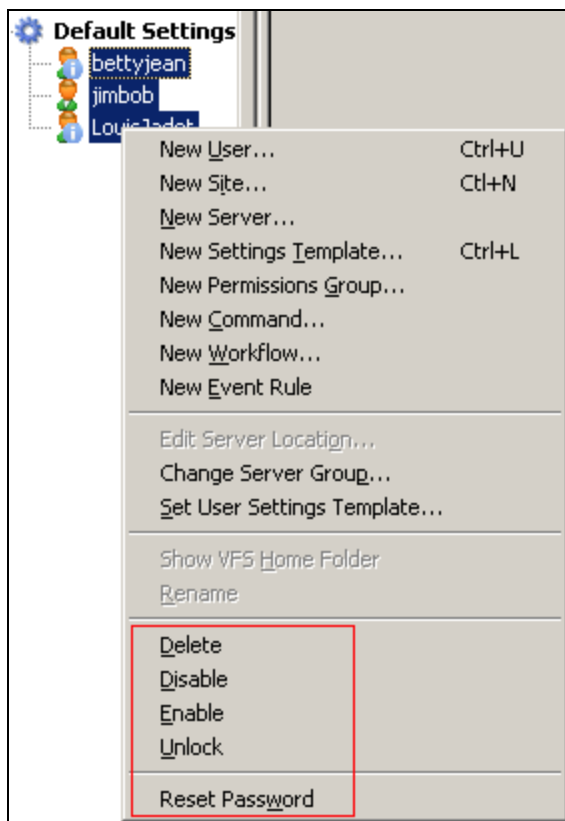
Managing Multiple User Accounts

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 Disk Quota

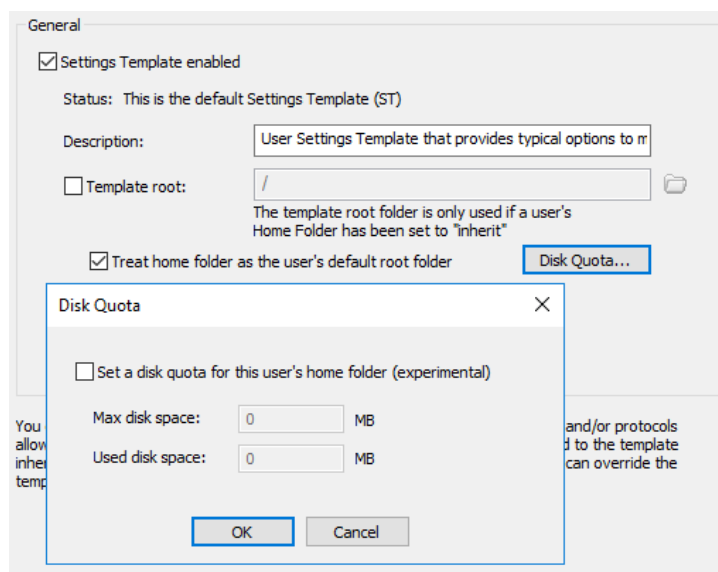
Disk space management is an important aspect of server administration. Setting quotas allows you to specify the maximum amount of disk space available to each user in their home folder.

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 [DiskQuotaBaselineCalculationFrequencyInDays](#) allows 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.

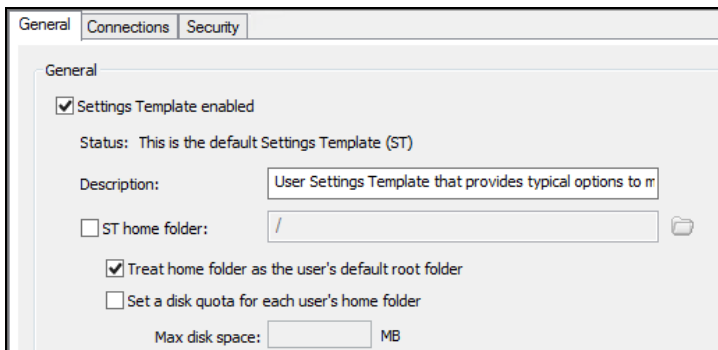
For Sites that use NTLM/AD authentication, if the user account has a Home Folder defined by the AD administrator, then EFT's VFS will **not** create a physical folder for the new user, but instead creates a virtual folder that points to the path specified in Active Directory for the home folder for that 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 Site](#) are 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:

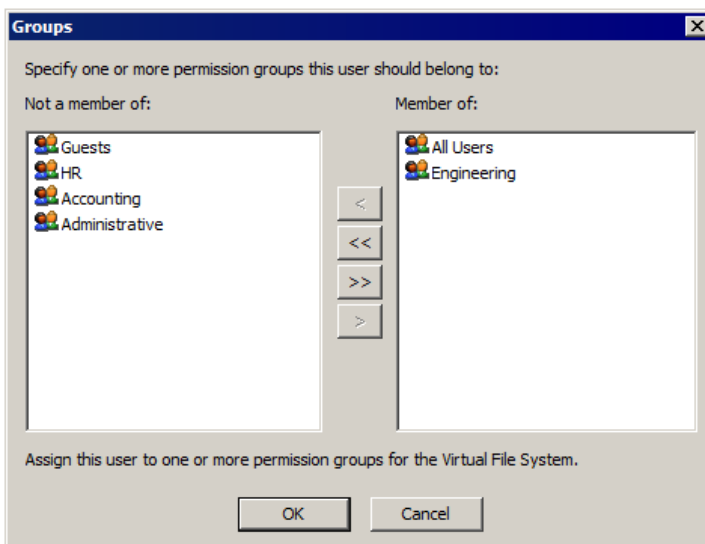
- Select the **Treat home folder as default root folder** check box to make the home folder the user's root folder. If the check box is selected, the user cannot browse above their home directory.
 - Clear the **Treat home folder as default root folder** check box. When it is cleared, if you built the 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 [Security](#) tab.
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.

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:

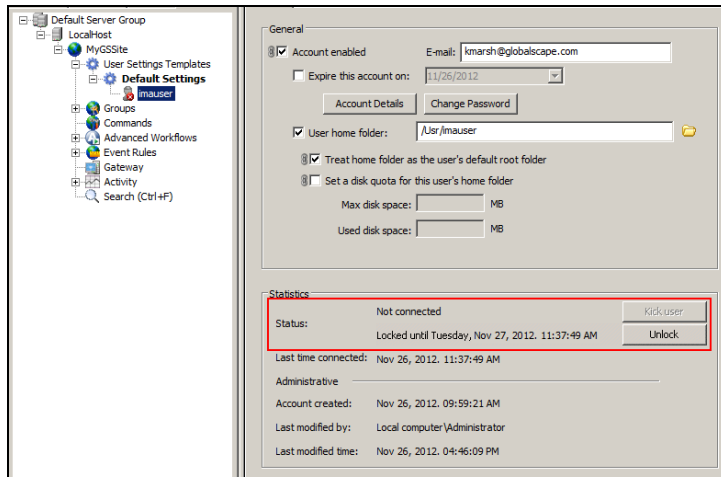
1. Open a user's properties in your AD management tool, click the **Profile** tab, and look at the **Home Folder** section.
2. Click **Connect**, select any appropriate drive letter, then in the **To** box provide the desired UNC path. The UNC path will be used when creating your new AD Authentication 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.

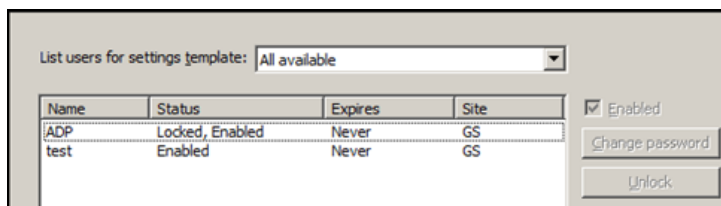
Unlocking a User Account

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 Details](#) dialog 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 [General](#) tab.

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 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.

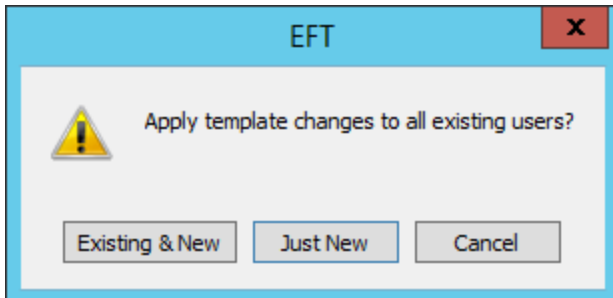
(Changes to the template only affect new users; existing users' settings will not be changed unless you reset the fields on the **User Account Details** dialog box for each of those users, as described [below](#).)

The image shows two side-by-side screenshots of the 'User Account Details Template' dialog box. Both windows have a title bar with the text 'User Account Details Template' and a close button (X). The left window shows a drop-down menu with 'Email' selected. Below the menu, there are six attributes with checkboxes: 'Display name:' (set to 'Email'), 'Default value:', 'Is personal data?' (checked), 'Is modifiable?' (checked), 'Is enabled?' (checked), and 'Is visible to user?' (checked). At the bottom are 'OK' and 'Cancel' buttons. The right window shows a drop-down menu with 'Comments' selected. Below the menu is a list of fields: 'Email', 'Full Name', 'Company Name', 'Mobile', 'Description', 'Phone', 'Fax', 'Pager', 'DUNS', 'Partner ID', 'Custom 1', 'Custom 2', 'Custom 3', and 'Comments'. The 'Comments' field is highlighted at the bottom of the list.

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 image shows two screenshots of the 'User Account Details' dialog box. The left screenshot is titled 'User Account Details Template' and contains a list of fields with their attributes. The 'Display name' field is highlighted with a red box, and its value is 'Bldg. #'. The right screenshot is titled 'User Account Details for lmauser1' and shows the same fields as the template. The 'Bldg. #' field is highlighted with a red box, and a red arrow points from the 'Display name' field in the template to this field in the user details 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.

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**.

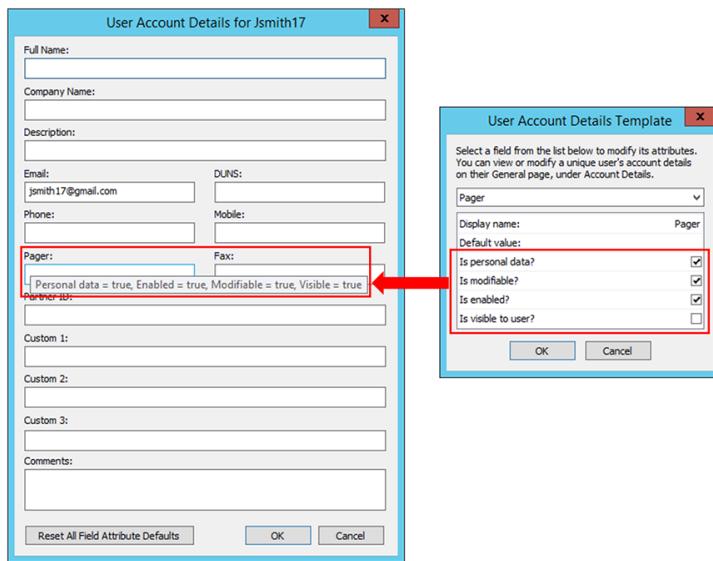
The default setting (true or false) for each field are shown in the table below:

FieldName	Email	Full Name	Company Name	Mobile	Description	Phone	Fax	Pager	DUNS	Partner ID	Custom1	Custom2	Custom3	Comments
Display name	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Is Personal data?	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Is Modifiable?	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Is Enabled?	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
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**

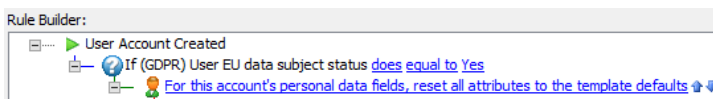
Field Attribute Defaults to make the field attributes in the **User Account Details** dialog box match the template's settings.



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.

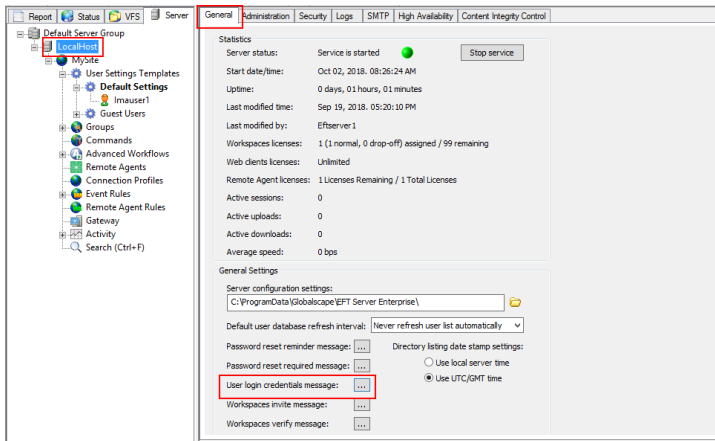


User Login Credentials Message

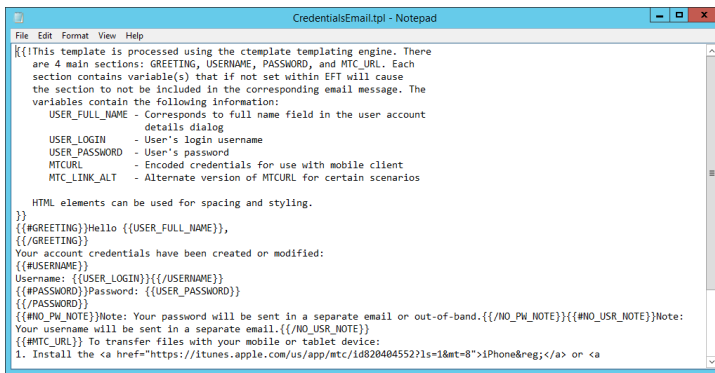
When you create a user, you have the option of sending the user an [email that contains the login credentials](#) for connecting to EFT. You can configure the content of the email to apply to all users.

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

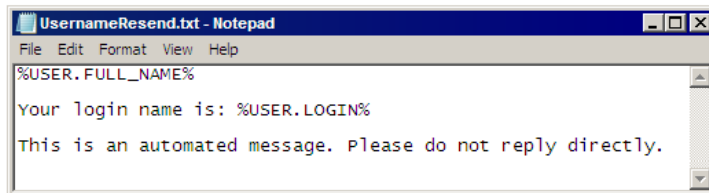
1. Make a copy of the existing template.
 2. Make your edits (using a text editor, such as Notepad), being careful not edit any of the variables or necessary code.
 3. Save the edited version with the Site name and an underscore prepended to the front of the filename. For example, name it `MyFrenchSite_CredentialsTemplate.tpl`.
6. Click **Apply** to save the changes on EFT.
7. Restart the Site so it can read in the new template.

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.

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.

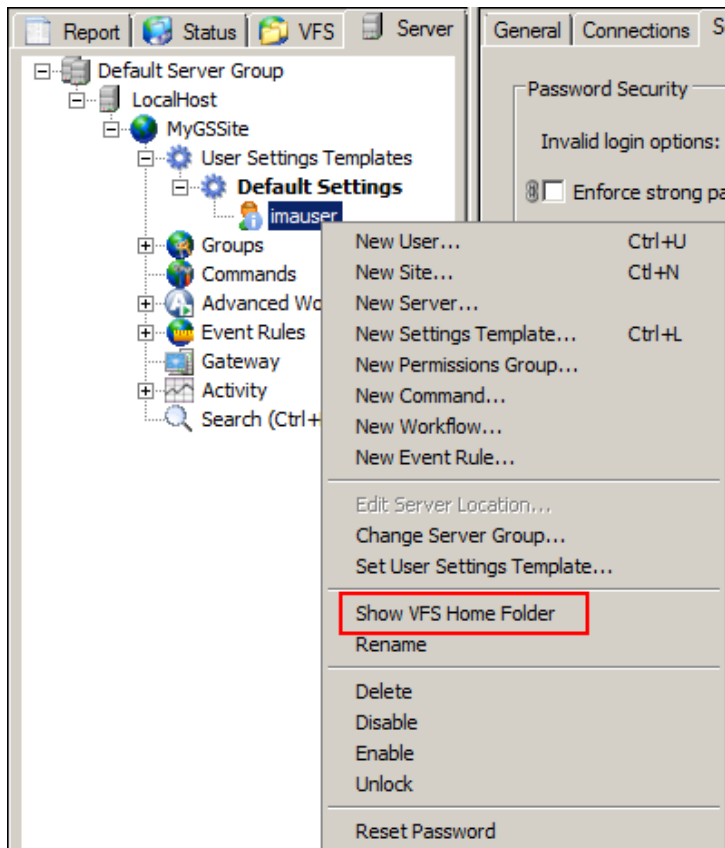
Viewing a User's Home Folder

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

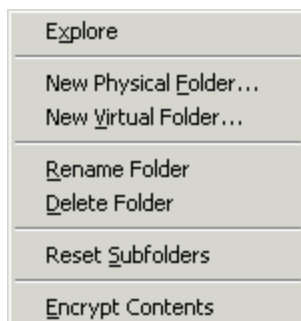
1. In the administration interface, [connect to EFT](#) and click the **Server** tab.
2. On the **Server** tab, right-click the user account whose folder you want to view, and then click **Show VFS Home Folder**.



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**.



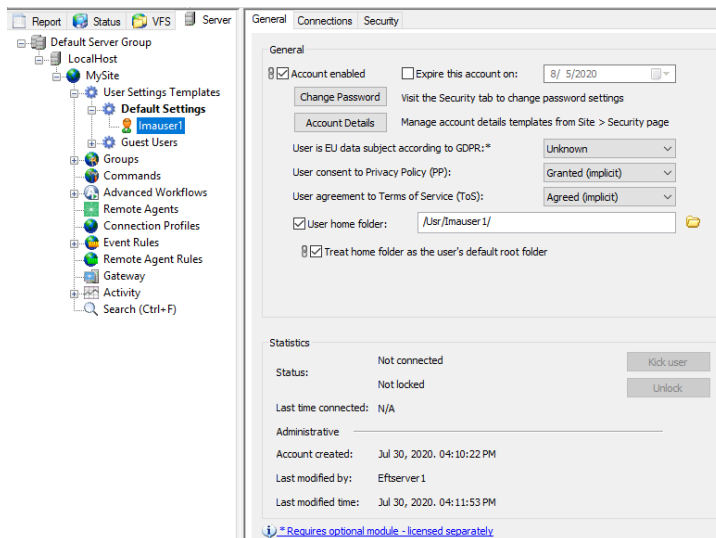
3. Windows File Explorer opens with that user account's home folder selected.

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.

Password Security Settings

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>.

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](https://kb.globalscape.com/KnowledgebaseArticle10516.aspx).

- 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.)

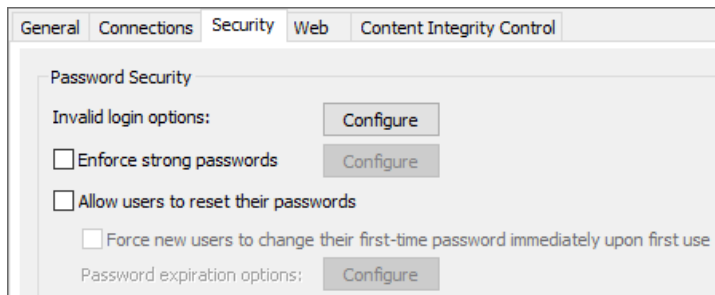
There is no way to ask FTP users to change their password prior to logging in. We must allow them to actually login (authenticate) but then prevent any further interaction with their session until they change their password.

- 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.)

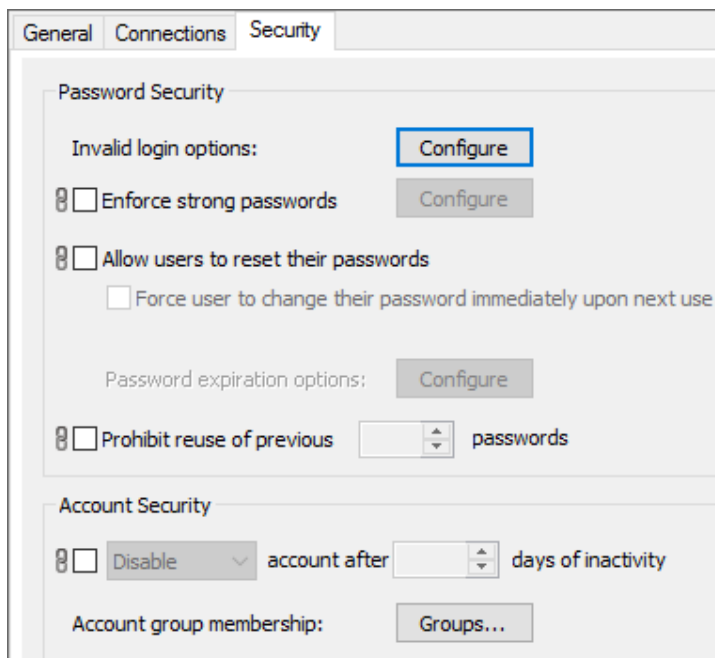
You can configure password reset on the Site, Settings Template, and for each user. (The Site setting **Force new users to change their first-time password immediately upon first use** is inherited by the Settings Templates.)

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 reset 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.

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 [General](#) tab.
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.

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 complexity](#) and 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)

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.

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
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.

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 [Security](#) tab.
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.**

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.

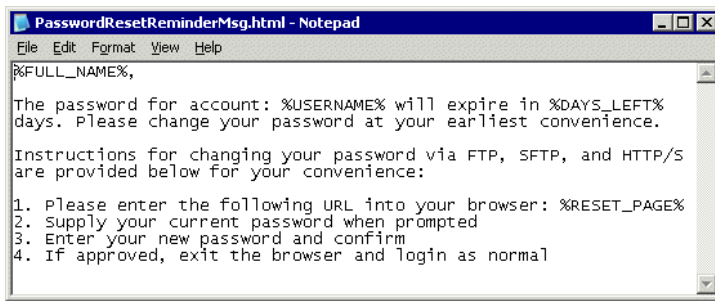
The files are stored in **C:\ProgramData\Globalscape\EFT Server\Templates** directory (by default) and apply to all Sites on the Server. You can also create Site-specific versions (described below).

You can define how long password reset links 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.

- Next to **Password reset reminder message**, click the browse icon. Your default text editor (for example, Notepad) opens with the reminder text.

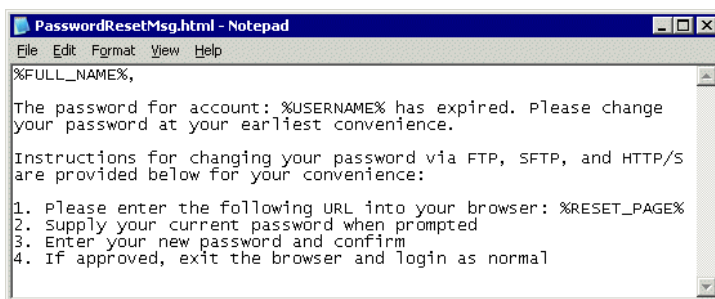


```

PasswordResetReminderMsg.html - Notepad
File Edit Format View Help
%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

```

- 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.
- Next to **Password reset required message**, click the browse icon . Your default text editor, usually Notepad, opens with the reminder text.

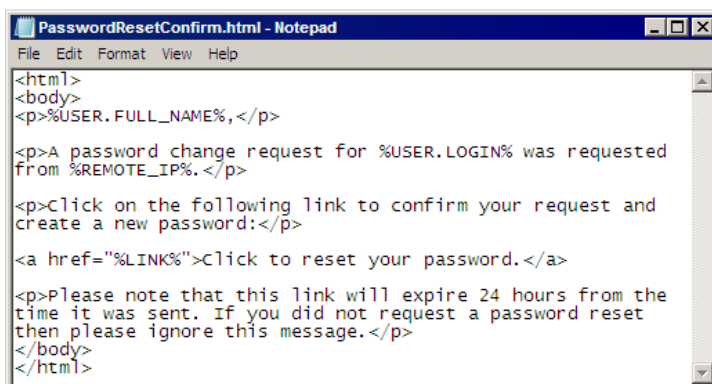


```

PasswordResetMsg.html - Notepad
File Edit Format View Help
%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

```

- 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.
- To edit the **Password reset confirmation message**, open the file in your default text editor, usually Notepad.



```

PasswordResetConfirm.html - Notepad
File Edit Format View Help
<html>
<body>
<p>%USER.FULL_NAME%,</p>
<p>A password change request for %USER.LOGIN% was requested
from %REMOTE_IP%.</p>
<p>Click on the following link to confirm your request and
create a new password:</p>
<a href="%LINK%">Click to reset your password.</a>
<p>Please note that this link will expire 24 hours from the
time it was sent. If you did not request a password reset
then please ignore this message.</p>
</body>
</html>

```

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`

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 screenshot shows the 'Security' tab of the EFT configuration interface. It is divided into three main sections:

- Password Security:**
 - Invalid login options: [Configure]
 - ☐ Enforce strong passwords [Configure]
 - ☐ Allow users to reset their passwords
 - ☐ Force new users to change their first-time password immediately upon first use
 - Password expiration options: [Configure]
 - ☐ Suppress "Forgot Password" option (LDAP enabled sites only) for: All Domains
 - ☐ Prohibit reuse of previous 4 passwords
 - ☒ Persist username and password credentials for use in Event Rule context variables
 - ☒ Enable option to e-mail users their login credentials
 - ☒ e-mail both username and password together
 - ☐ e-mail the username and password in separate e-mails
 - ☐ e-mail the username only
- Account Security:**
 - ☒ Automatically create a home folder for new users
 - ☒ Grant full permissions to users in their home folder
 - ☐ Disable account after 90 days of inactivity
 - [User Account Details Template...]
- Data Security:**
 - Banned file types: [Configure]
 - OpenPGP security: [Configure]
 - Secure data removal: [Configure]
 - Encrypted folders: [Configure]
 - Secrets module: [Configure]

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.

- 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.

Password Expiration

Password expiration options:

☒ Expire passwords in 90 days

☒ Send user an e-mail upon expiration

☒ Remind 5 days prior to expiration

☒ Send user an e-mail prior to expiration

NOTE: The e-mail reminder and expiration message can be modified on the Server -> General tab.

OK Cancel

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.

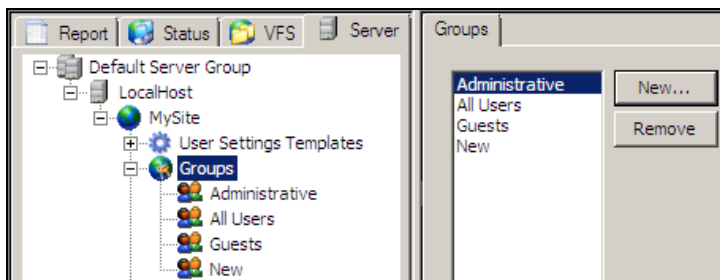
For all protocols, if the user's password is scheduled to expire, the email reminder is enabled, and the user account has an email address associated with it, an email will be sent informing the user of the pending expiration and provides instructions on how to change the password for one or possibly 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](#).

Controlling Access to Folders (Permission Groups & 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.)

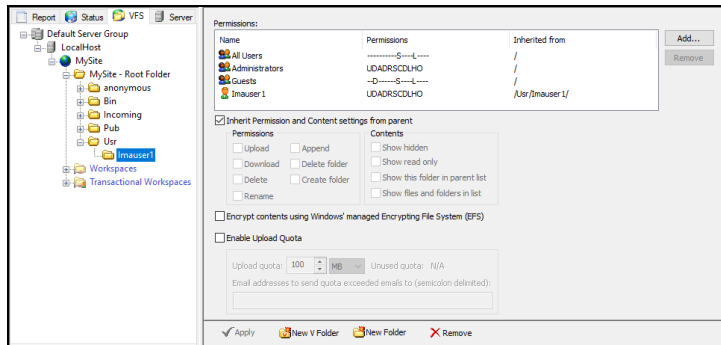


To specify user permissions

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.

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.

☒ Inherit Permission and Content settings from parent	
Permissions ☐ Upload ☐ Download ☐ Delete ☐ Rename ☐ Append ☐ Delete folder ☐ Create folder	Contents ☐ Show hidden ☐ Show read only ☐ Show this folder in parent list ☐ Show files and folders in list
☐ Encrypt contents using Windows' managed Encrypting File System (EFS)*	

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.

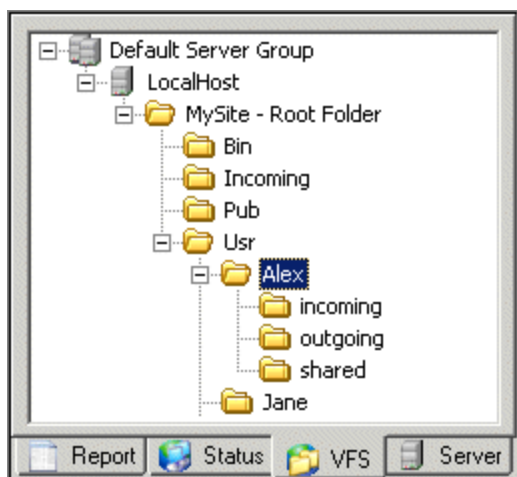
Contents

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.

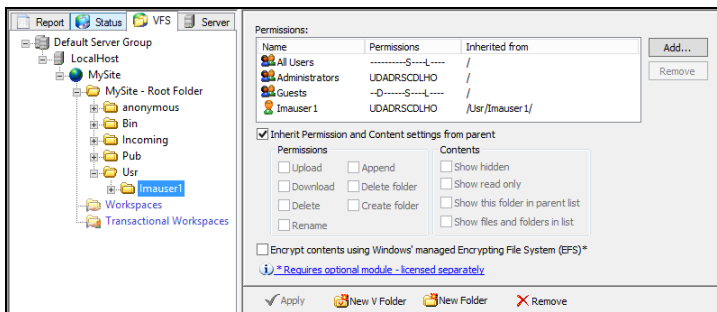
- The **Show files and folders in list** permission applies to both files and folders in the selected directory.
- The **Show this folder in parent list** permission applies to the visibility of the selected folder in its parent directory.
- Default inheritance rules will cause the subfolders of a **Show this folder in parent list**-disabled folder to not display.

Adding a User or Group to VFS Permissions

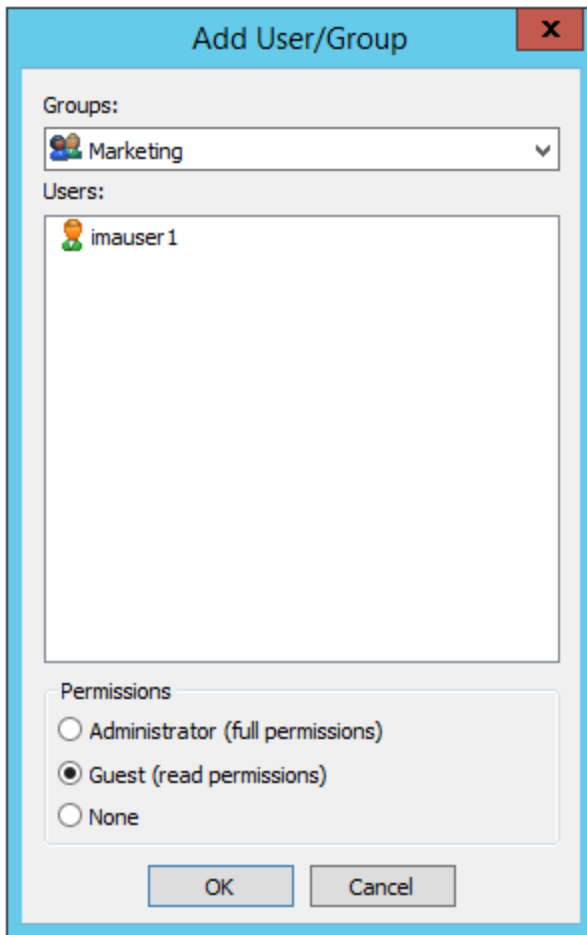
You can add a user or Group to existing permissions on the **VFS** tab's **Permission** pane. The **All Users**, **Administrators**, and **Guests** Groups are default Groups created by EFT during installation. You can create other Groups on the **Server** tab. Refer to [Permission Groups](#) for more 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

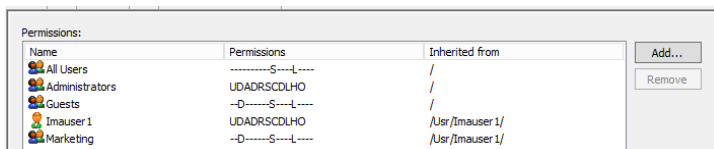
1. In the administration interface, [connect to EFT](#), and then click the **VFS** tab.
2. In the left pane, click the folder you want to configure. The right pane displays each of the users and Groups who have permissions on the selected folder.



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.

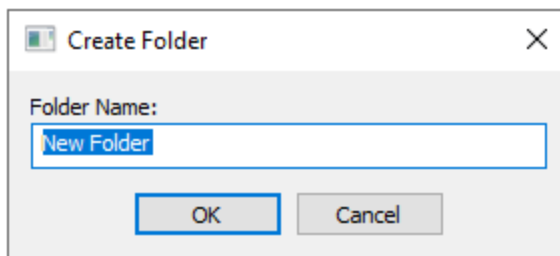
Creating a New Physical Folder

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.

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.

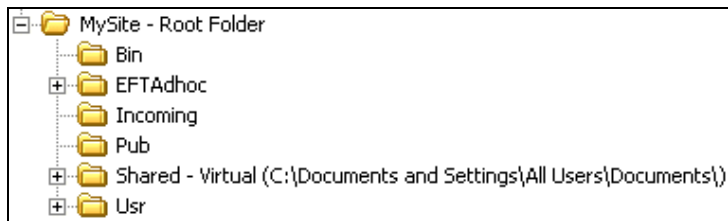
3. In the **Alias** box, type a name for the folder. For example, type `Shared`.
4. In the **Type** box, specify whether the folder is **Local/LAN** or **Cloud Storage**.

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.

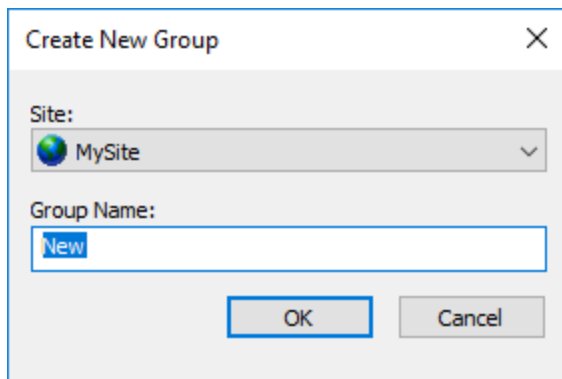
Creating Permission Groups

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.

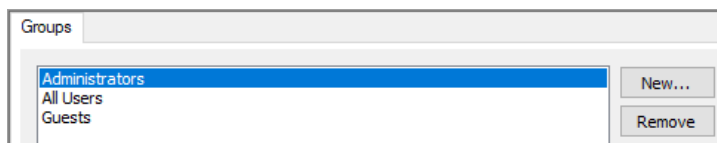
Refer to [Adding or Removing Users to or from a Group](#) and [The Virtual File System](#) for information about users' permissions in relation to their assigned Group(s).

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.

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**.

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**.

Disabling Inheritance in the VFS

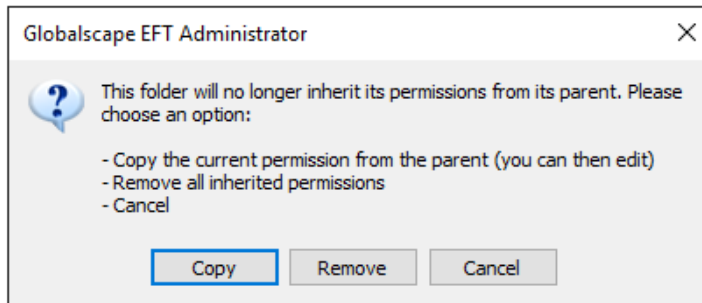
You can override a user's inherited settings by clearing the **Inherit permissions from parent folder** check box. If you later decide you want the folder to inherit permissions again, simply select the **Inherit permissions from parent folder** check box.

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

Encryption in EFT

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).

- **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 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 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 be 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 be decrypted with `eftencrypt.exe`. Use `eftencrypt.exe <key> <path to target file>` to run the decryption process, and then the 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 result 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.

Encrypted Folders

EFT server will encrypt files in the specified folders as they arrive over supported protocols, and decrypt files when departing over those same protocols. The server will also encrypt files that are downloaded (as client) into an encrypted folder, and decrypt files that are copy/moved to a different location.

Path	Key Alias

Add

Remove

Secret key:

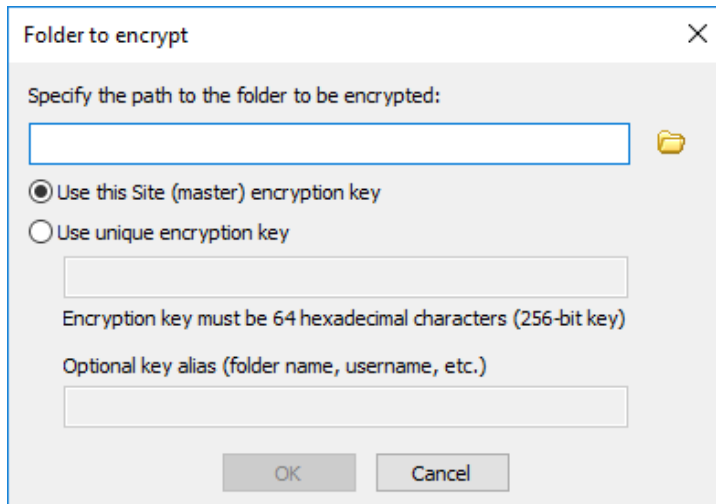
.....

This secret was randomly generated by EFT. As a security and business continuity best practice, we recommend that you change the secret and maintain a copy of the secret in your key manager for safekeeping. Please contact your account rep or refer to EFT's help file for instructions on how to properly replace the default secret.

Cancel Apply OK

- 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.



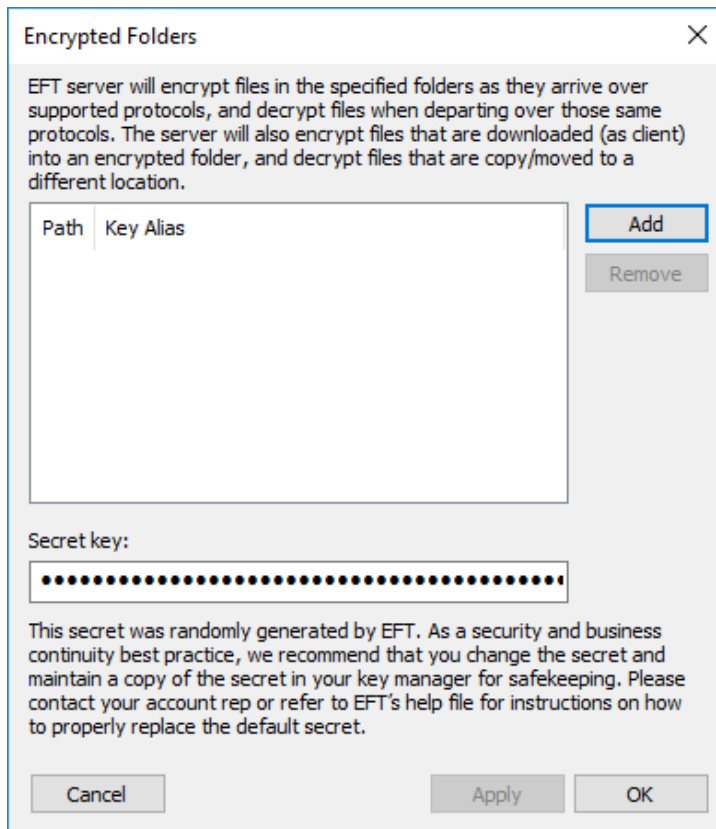
6. Type or browse for the folder that you want to encrypt. You can only encrypt the folders in the Site's root folder (for example, C:\InetPub\EFTRoot\MySite). (See [note above](#) regarding clusters.)
7. Click one of the following:
 - **For the Site encryption key**, click **Use this Site (master) encryption 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**.

Enabling EFS Encryption

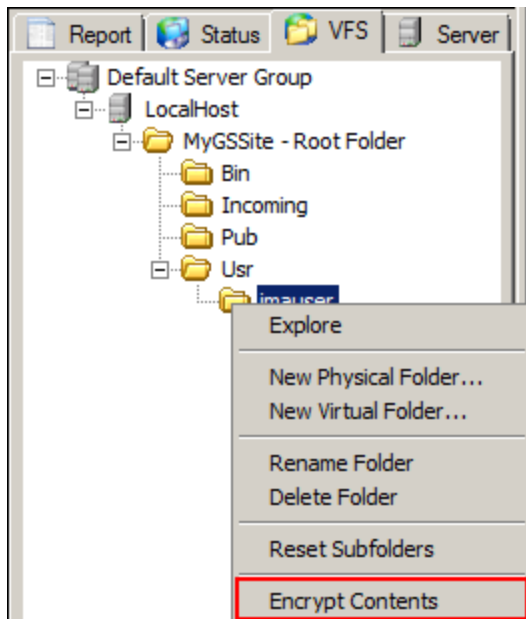
Physical folders stored on the disk in EFT's Virtual File System (VFS) can be transparently encrypted during read/write using Microsoft's Encrypting File System (EFS) by which data is encrypted as it is written to disk, and decrypted prior to transmission.

- 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

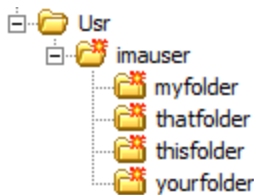
1. In the administration interface, [connect to EFT](#) and click the **VFS** tab.
2. In the left pane, right-click the parent folder you want to configure, and then click **Encrypt Contents**.



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**.

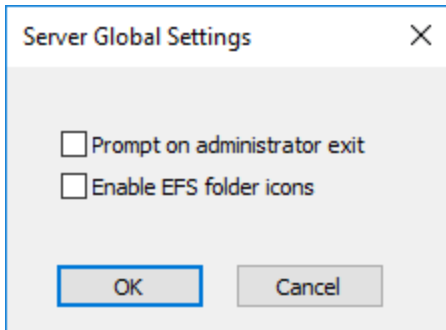
Enable EFS Folder Icons

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.)

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.

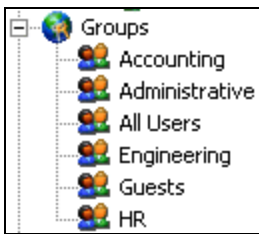
Virtual folders that point to a drive other than C: or a UNC share are visible using the MLSD FTP command.

Renaming a Group

When you rename a permission Group, all references to the Group are also updated.

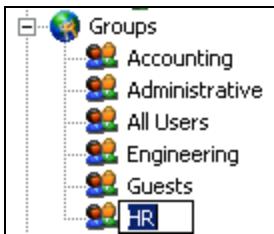
To rename a permission Group

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.

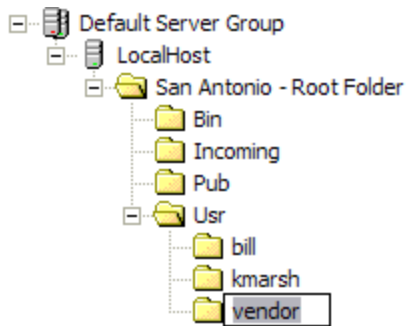
Renaming a Physical Folder

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

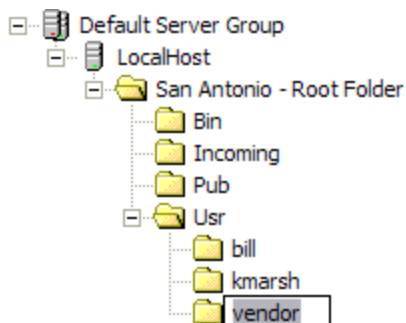
You can change the name of a virtual folder in the VFS tree.

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**.

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 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.

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.

The screenshot shows the VFS configuration window. On the left is a tree view of the file system structure. The main area is divided into 'Permissions' and 'Contents' sections. The 'Enable Upload Quota' checkbox is checked and highlighted with a red box. Below it, the 'Upload quota' is set to 100 MB, and the 'Unused quota' is N/A. The 'Email addresses to send quota exceeded emails to' field contains 'eftadmin@helpssystems.com'.

Name	Permissions	Inherited from
All Users	-----S---L----	/
Administrators	UDADRSDDLHO	/
Guests	--D-----S---L----	/
Imauser1	UDADRSDDLHO	/usr/Imauser1/

☒ Inherit Permission and Content settings from parent

Permissions	Contents
☒ Upload	☒ Show hidden
☒ Append	☒ Show read only
☒ Download	☒ Show this folder in parent list
☒ Delete	☒ Show files and folders in list
☒ Create folder	
☒ Rename	

☐ Encrypt contents using Windows' managed Encrypting File System (EFS)

☒ Enable Upload Quota

Upload quota: 100 MB Unused quota: N/A

Email addresses to send quota exceeded emails to (semicolon delimited):
eftadmin@helpssystems.com

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/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.

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\).

Getting Support

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](#).

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 Globalscape 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.

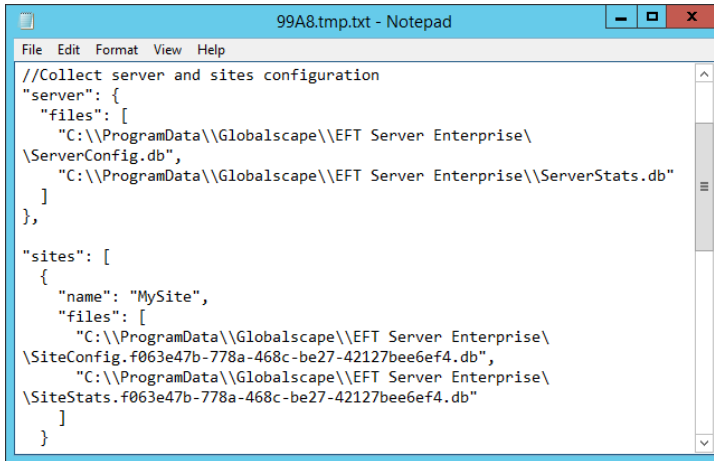
You can [install the EFT administration interface](#) on another computer that has Internet access, from which you can view and manage EFT, provided that computer can access the EFT computer remotely.

The Generate Support Data wizard automates the process of gathering key EFT and system configuration information to assist with support cases.

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.



The following data will be collected by default:

- Gathers all of the EFT SQLite DB files.
 - Generates system info
 - Gathers Windows application and system event logs (but ONLY for EFT application)
 - HKLM registry backup
 - Complete list of installed software
 - EFT log files (going back 1 day, by default)
 - FTP.cfg, .aud, and .bak files, if present
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 Policy](#) and 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. For example:

```
Starting collection process...
```

```
Collecting data...this may take a few minutes
```

```
Error in parsing manifest file (missing, corrupted?)
  <-if error, sample
```

```
Error due to timeout (600 seconds). Files locked
  or unavailable? <-if error, sample
```

```
Done
```

8. Click **Next**.

Generate Support Data

Run this utility to automate the process of gathering key EFT and system configuration information to aid ongoing support cases. We encourage you to view and optionally edit the file collection manifest and examine the generated dataset before sending it to us. You must read and consent to our privacy policy before you generate or submit EFT and system configuration information to Globalscape.

Optionally send collected data to Globalscape support:

Case: Pass:

Status

The support data file is ready. You can now submit it.

< Back **Finish** Cancel Help

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, 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}

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.