

# FORTRA



## Globalscape EFT v8.1.0 Installation 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.

202309180512

# Table of Contents

|   |           |
|---|-----------|
| <b>Introduction to EFT Managed File Transfer</b> .....      | <b>6</b>  |
| What's New in EFT? .....                                    | 9         |
| v8.1.0.16, June 5, 2023 .....                               | 10        |
| <b>Before You Begin</b> .....                               | <b>11</b> |
| Feature Availability .....                                  | 12        |
| System Requirements .....                                   | 23        |
| EFT (Server Service) Requirements .....                     | 23        |
| EFT Administration Interface Requirements .....             | 25        |
| Auditing and Reporting Module (ARM) Requirements .....      | 26        |
| AS2 Module Requirements .....                               | 27        |
| Web Transfer Client (WTC) and Workspaces Requirements ..... | 28        |
| Advanced Authentication Modes Module Requirements .....     | 28        |
| Regulatory Compliance Module (RCM) Requirements .....       | 29        |
| EFT Outlook Add-In Requirements .....                       | 29        |
| DMZ Gateway® Requirements .....                             | 29        |
| Advanced Workflow Module Requirements .....                 | 30        |
| Remote Agent Module (RAM) Requirements .....                | 30        |
| Mobile Transfer Client (MTC) System Requirements .....      | 30        |

Content Integrity Control Action Requirements ..... 30

EFT Specifications ..... 31

Safe Operating Limits ..... 32

EFT System Architecture ..... 32

**Installing EFT ..... 33**

    Installation Logging ..... 33

    Installing EFT, Administration Interface, and Modules ..... 34

    Installing the Advanced Workflow Module ..... 52

    Active-Active HA Cluster—Installing or Upgrading the Server ..... 53

    Active-Passive Failover Clustering--Installing or Upgrading ..... 53

**After You Are Done ..... 54**

    Configuration and Security Best Practices ..... 54

    Creating and Configuring an EFT Server ..... 55

    Configure the First EFT Connection ..... 56

    Activating the Software (Licensing EFT and Modules) ..... 69

    Registering EFT and the Modules ..... 71

    Windows Account for the EFT Server Service ..... 77

        Creating a Windows User Account for EFT ..... 79

        Set Windows NT Permissions for EFT ..... 79

        Assigning the Service to a Windows User Account ..... 82

---

|  |     |
|--|-----|
| HA Nodes Configuration Files .....                     | 82  |
| Installing the Administration Interface Remotely ..... | 84  |
| Backing Up or Restoring Server Configuration .....     | 88  |
| Modifying or Repairing the Installation .....          | 96  |
| Promoting EFT Stand-Alone to Cluster Node .....        | 97  |
| Upgrading EFT .....                                    | 98  |
| Upgrade HA Nodes with Zero Downtime .....              | 106 |
| Uninstalling the Software .....                        | 113 |

# 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)** - 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<sup>®</sup>** - used in combination with EFT to create a multi-tier 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/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. In v8.0.7 and later, this module 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. This module is also needed, along with the ARM, to run administrator activity reports and privacy reports.
- **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<sup>®</sup>](#).
- **Timer Event Module (TEM)** - Allows you to execute a specified Action only one time or repeatedly at specified intervals. For example, you could schedule an Action (for example, generate and send a report) to occur on July 8 at midnight, or every Monday morning, or on the last Friday of every month at 2 a.m.
- **Workspaces** - Allows you to share folders and their files with internal and external users.

**Additional tools (license required):**

- [Business Activity Monitoring \(BAM\)](#) is a web-based dashboard tool that uses data from the Auditing and Reporting module to provide full visibility into the flow of data through your EFT system. Evaluate data trends over time and gain instantaneous knowledge about the current state of your system.

## What's New in EFT?

Below is a **high-level summary** of changes in this version of EFT, with links to relevant help topics. **For a detailed log of changes and fixes, refer to the release notes in the [Client Success Portal](#).**

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

Review [Upgrading the Software](#) and the [Upgrading EFT](#) knowledgebase article before upgrading.

Refer to the [COM API Reference](#) for details of changes to the COM API.

## v8.1.0.16, June 5, 2023

### Fixes

#### EFT Event Rules

- Fixed an issue where EFT event rules configured with Matching Filenames set to Numerate on local file uploads would not numerate the initial file properly.

#### EFT Security Updates

- Mitigated a directory traversal vulnerability known as "Zip Slip" when exercising compression or decompression within EFT. Refer to KB article <https://kb.globalscape.com/Knowledgebase/11585/Is-EFT-susceptible-to-the-Zip-Slip-vulnerability>.
- Mitigated an EFT administrator authentication out-of-bounds memory read vulnerability. Refer to KB article <https://kb.globalscape.com/Knowledgebase/11586/Is-EFT-susceptible-to-the-Authentication-Bypass-via-Outofbounds-Memory-Read-vulnerability>.
- Mitigated an EFT server crash due to vulnerability when sending recursively compressed packet to the administrator port. Refer to KB article <https://kb.globalscape.com/Knowledgebase/11588/Is-EFT-susceptible-to-the-Denial-of-service-via-recursive-Deflate-Stream-vulnerability>.
- Setting "Require SSL for remote administration" as default when enabling remote administration to avoid password leak due to insecure defaults. Refer to KB article <https://kb.globalscape.com/Knowledgebase/11587/Is-EFT-susceptible-to-the-Password-Leak-Due-to-Insecure-Defaults-vulnerability>.
- [Multifactor authentication](#) (2FA, SMS) has been moved to the HTTPS module

# Before You Begin

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

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

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

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

## Before installation

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

# Feature Availability

**NOTE:** Please refer to the topic "[EFT Arcus Features](#)" in the Globalscape Knowledgebase if you are comparing EFT on-premises to EFT Arcus.

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

## Core Features of EFT

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

|  |
|--|
| Active-Active clustering (HA)  |
| Active-passive clustering (Failover for high availability)                   |
| Administrative console   |
| Admin roles and permissions  |
| Audit performance counters to Windows Perfmon                                |
| Auditing to text file  |
| Auditing internal metrics to local database                                  |
| Backup and restore wizard  |
| Ban file types by extension  |
| Batch management of users  |
| Built-in, NTLM, AD, and LDAP auth (including AD admin auth)                  |
| COM API  |
| Connection Profiles (requires HTTPS, SFTP, or FTPS to connect as the server) |
| Content Integrity Control (CIC)  |
| Delegated administration   |
| Denial of server and flood protection  |
| Else conditional logic in rules  |
| Encrypted folders (secure data at rest)                                      |

|  |
|--|
| Expire inactive accounts (including admin accounts)  |
| Expire passwords after N days (including admin accounts)   |
| Expiration reminder  |
| FIPS 140-2-certified crypto (requires SSL/TLS or SFTP)   |
| FTP plain (FTPS requires FTPS module)  |
| IP white/black listing   |
| Mobile file transfer   |
| Override VFS credentials   |
| Password complexity  |
| Performance counters   |
| REST-based administration  |
| Reusable connection profiles   |
| Run command-line scripts   |
| SSL client cert auth (full functionality available only when HTTPs or FTPs module is registered)   |
| Triggers based on incoming (uploaded) files  |
| Virtual folders mapped to shares   |
| Windows EFS encryption   |
| Event Rule Actions: <ul style="list-style-type: none"><li>• File scan for DLP/AV, ICAP/CIC</li><li>• Flow: Stop Processing</li><li>• Flow: Variable</li><li>• Protocol: Email</li><li>• System: Backup</li><li>• System: Cleanup</li><li>• User: Action</li><li>• Windows: Event Log</li></ul> |

Event Rules:

- "IF" conditional for triggers
- Create a change log for rules
- "Else" conditional for triggers
- Event Rule import/export
- Group triggers into folders (Event Rule Folders)
- Securable objects (Event Rule Permissions)
- Connection Events (all)
- File Server Events (all)
- Server Events (all)
- Site Events (all)
- User Events (all)

## Features by Category

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

|   |                                    |
|---|------------------------------------|
| AAMM = Advanced Authentication Modes Module | FTPS = FTPS module                 |
| ARM = Auditing and Reporting Module         | HTTPS = HTTPS module               |
| AS2 = AS2 protocol module                   | PGP = PGP Module                   |
| AWM = Automate Workflow Module              | RAM = Remote Agent Module          |
| BAM = Business Activity Monitoring          | RCM = Regulatory Compliance Module |
| CCM = Cloud Connector Module                | SFM = Secure Forms Module          |
| DMZ = DMZ Gateway                           | SFTP = SFTP module                 |
| EAM = Enterprise Actions Module             | TEM = Timer Event Module           |
| FMM = Folder Monitor Module                 | WMU = Workspaces                   |
| FTC = File Transfer Client                  |                                    |

## Protocols

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

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

### Authentication (Access Controls)

| Feature  | Core or module |
|--|----------------|
| <a href="#">EFT-managed</a> accounts (i.e., "built-in authentication, or Globalscape authentication)   | Core           |
| <a href="#">Active Directory</a> (AD) – native Windows integration, including admin accounts)<br><br>(In EFT Arcus, "AD impersonation" is available, but not authentication.)                | Core           |
| <a href="#">ODBC</a> - leverage any ODBC data source   | Core           |
| <a href="#">LDAP</a> - authenticate against LDAP sources, including AD   | Core           |
| <a href="#">SAML (WebSSO)</a> - including <a href="#">Just In Time (JIT) provisioning</a>  | AAMM           |
| <a href="#">RADIUS</a> - often used as a two-factor authentication source  | AAMM           |
| <a href="#">RSA SecurID</a> <sup>®</sup> (native and Steel-Belted Radius (SBR))  | AAMM           |
| <a href="#">CAC</a> - Common Access Card authentication  | AAMM           |
| Secrets module   | CCM            |
| <a href="#">SMS authentication</a> - two-factor authentication (2FA) for <a href="#">WTC and Workspaces</a><br><br>(In EFT Arcus, the "out-of-ban0d" passcode to pick up files is available. | HTTPS          |

### Authorization (Resource Controls)

| Feature   | Core or module |
|---|----------------|
| AD Impersonation - Active Directory manages permissions | Core           |

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

## Administration

| Feature  | Core or module |
|--|----------------|
| <a href="#">Silent installation - unattended setup</a> | Core           |

| Feature  | Core or module |
|--|----------------|
| <a href="#">Administrator GUI</a> - Windows based Graphical User Interface (GUI)   | Core           |
| <a href="#">Remote administration</a> - administrate from other systems in the network   | Core           |
| Secure remote administration - SSL encrypted administration communications   | Core           |
| <a href="#">Multiple administrators</a> - allow concurrent administration  | Core           |
| <a href="#">Secure administration</a> - same password complexity options available for administrators as for users                                   | Core           |
| <a href="#">Flexible authentication</a> - leverage native, NTLM, or AD to authenticate administrators  | Core           |
| <a href="#">Forensics</a> - audit and report on all administrator activity and changes   | ARM            |
| <a href="#">COM API</a> - programmatic administration  | Core           |
| <a href="#">REST endpoint</a> for querying administrative info and server status   | Core           |
| <a href="#">Backup and Restore</a> - one-click backup and easy restore of entire configuration<br><b>(Scheduled backups requires the TEM)</b>        | Core           |
| <a href="#">Batch account management</a> - perform actions to multiple accounts simultaneously (such as multi-select users to reset their passwords) | Core           |
| Specify <a href="#">personal data and privacy settings</a> on a Site and per user  | RCM            |
| Generate <a href="#">GDPR DPIA report</a>  | ARM / RCM      |

## Auditing and Visibility

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

## Automation (Integration with Other Systems)

| Feature  | Core or module |
|--|----------------|
| <a href="#">Event Rules change log</a>   | Core           |
| <a href="#">Group Event Rules into folders</a>   | Core           |
| <a href="#">React to stimuli</a> - trigger workflows based on file uploads and other server events   | Core           |
| <a href="#">Send email</a> to users or administrators as part of a workflow  | Core           |
| <a href="#">"Stop processing if failed" action</a>   | Core           |
| <a href="#">"If" and "Else" Conditions</a> in Event Rules  | Core           |
| <a href="#">Connection Events</a>  | Core           |
| <a href="#">Import/Export Event Rules</a>  | Core           |
| <a href="#">Context variables</a> - use transaction values inside of workflows   | Core           |
| <a href="#">Conditional logic</a> - build fine-grained business logic into workflows   | Core           |
| <a href="#">Backup Action</a> - Back up files ( <b>Scheduled backups requires the TEM</b> )  | Core           |
| <a href="#">Cleanup Action</a> - securely remove old files based on your organization's data retention policies ( <b>Scheduled cleanup requires the TEM</b> )  | Core           |
| <a href="#">Upload</a> and <a href="#">download</a> - push or pull files to remote servers as part of a workflow   | FTC            |
| <a href="#">User Account Action</a> - for tasks like re-enabling user accounts and compliance requests (for example, HIPAA, GDPR) in which users might ask that an organization remove all traces of their account.  | Core           |
| <a href="#">Windows Event Log Action</a>   | Core           |
| Create reusable <a href="#">connection profiles</a> for use in Event Rules   | Core           |
| <a href="#">Integration with antivirus and DLP</a> (Data Loss Prevention) tools to permit or prevent transfers based on policies.  | Core           |
| <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>◦ <b>Content Integrity Control</b> is used in event rules to send a file to an external antivirus scanner or data loss prevention solution for processing.</li> <li>◦ Customer must install an antivirus/ data loss prevention solution. Any third-party content inspection product that supports ICAP can communicate with the Content Integrity Control in EFT.</li> <li>◦ EFT Arcus has built-in Windows Defender antivirus protection at the OS level.</li> </ul> | Core           |
| <a href="#">File Server Events</a>   | Core           |

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

## Person-to-Person (P2P) File Transfer

| Feature   | Core or module          |
|---|-------------------------|
| Ad hoc file transfer – Allow authorized users to share files or folders with guest users via <a href="#">Outlook</a> or using the EFT web interface, for secure P2P file exchange | HTTP/S, Workspaces      |
| Two-way file sharing - recipients provided with multiple methods to securely send files to each other   | HTTP/S, Workspaces      |
| Receipt notification - email notification when files are picked up by the recipient   | HTTP/S, Workspaces      |
| <a href="#">Pick-up</a> authentication - recipients can be required to verify their identity before downloading files   | HTTP/S, Workspaces      |
| Full file tracking - Users and administrators can view complete history of files sent and received  | HTTP/S, Workspaces      |
| Centralized policy controls - administrator can set defaults and mandate policies or let authorized users decide  | HTTP/S, Workspaces      |
| Mixed mode authentication - optionally authenticate internal employees against AD, while maintaining guest isolation  | HTTP/S, Workspaces      |
| Integration with EFT - monitor all ad hoc file transfer activity from EFT   | HTTP/S, Workspaces      |
| <a href="#">Request files</a> – Authorized users can generate a request link that guests follow to securely upload files.   | HTTP/S, Workspaces      |
| Drop-off files to internal users with no attachment limits  | HTTP/S, Workspaces      |
| Manage personal data and <a href="#">privacy settings</a> for GDPR and other privacy rules in the Workspaces client   | HTTP/S, Workspaces, RCM |
| <a href="#">Multifactor authentication</a> via email or SMS for client logins   | HTTP/S, Workspaces      |
| Gather metadata for uploads in the client via <a href="#">upload forms</a>  | HTTP/S, Workspaces, SFM |
| View <a href="#">sent</a> and <a href="#">received</a> messages <a href="#">history</a> in client   | HTTP/S, Workspaces      |

## Architecture

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

# System Requirements

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

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

## EFT (Server Service) Requirements

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

- Operating systems:
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows 10 (administration interface only)
- Free RAM:
  - **Minimum:** 4 GB free RAM
  - **Recommended:** 8 GB free RAM (moderate [Advanced Workflows](#) usage)
  - **High Performance:** 16GB free RAM (if [Advanced Workflows](#) are used extensively)
  - More RAM could be required for large file transfers over the AS2 protocol. AS2 transfers can use up to 40% of the Server's RAM.
- CPU:
  - **Minimum:** Dual-core CPU of at least 2.5GHz (for minimal processing/ automation)
  - **Recommended:** Quad-core, at least 2.5 GHz (for moderate processing/automation)

- **High Performance:** 8+ cores, at 2.5 GHz (for high amount of processing/automation)
- Microsoft .NET Framework 4.0
- EFT requires the following dependencies:
  - Microsoft ODBC Driver 17 for SQL Server (used for SQL ARM)
  - Microsoft OLE DB Driver for SQL Server (used for SQL ARM)
  - Microsoft Visual Studio C++ 2010 x64 Redistributable – 10.0.30319
  - Microsoft Visual Studio C++ 2015-2022 Redistributable (x64) – 14.31.31103
  - Microsoft Visual Studio C++ 2015 -2022 Redistributable (x86) – 14.31.31103
- Max Latency (measured while not under load):
  - EFT to network share: <25ms
  - EFT to SQL/Oracle database: <10ms
  - EFT to DMZ Gateway: <50ms
  - EFT to Auth manager: <25ms
- **For HA (active-active) installations:**
  - Microsoft Message Queuing (MSMQ) must be installed.
  - Load balancer, such as F5® BIG-IP® Local Traffic Manager
  - File share (SMB or CIFS) for EFT configuration and users' files accessible via UNC path is required (configured as High Available storage for redundancy is recommended)
  - If file replication technology is used for Disaster Recovery, it must be configured as synchronous file replication. Technologies that use asynchronous file replication are not supported.
  - Fully qualified domain name (FQDN) or DNS record for File Shares and Databases is required and best practice
  - If *encryption at rest* is required, determine whether your storage vendor's solution includes built-in encryption or supports [Microsoft's Encrypted File Shares \(EFS\)](#). If neither option is available, you can leverage EFT built-in [Encrypted Folders](#) feature,

which is available in standalone or high availability (HA) configurations.

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

## EFT Administration Interface Requirements

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

- Windows 10, 11, 2016, 2019
- 1 GB of free RAM
- 1280x800 resolution or higher display
- Microsoft Windows Installer 4.5
- Microsoft .NET Framework 4.0 and later

## Auditing and Reporting Module (ARM) Requirements

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

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

EFT is supported with the following SQL Server version:

- SQL Server 2019
- SQL Express 2019 (bundled in EFT installer for evaluation purposes only)
- Microsoft® ActiveX Data Objects (ADO)
  - EFT uses Microsoft ActiveX Data Objects (ADO) 2.7 or later to handle database communication, which in turn should load the Oracle drivers to handle Oracle implementation details. How and what is connected largely depends upon the connection string. By default (if you do not supply the entire connection string in EFT), the Oracle connection string should look like:

```

Provider=OraOLEDB.Oracle.1;
Data Source=(DESCRIPTION =

    (ADDRESS_LIST = (ADDRESS
    = (PROTOCOL = TCP) (HOST = {host value}) (PORT
    = {port}))) "

    (CONNECT_DATA = (SERVICE_NAME
    = {database name}));

Persist Security Info=true;PLSQLRSet=1;PwdChgDlg=0;User
Id={username};Password={password};

```

- Refer to Oracle's documentation regarding [Oracle system requirements](#). Be sure to reboot after you install the Oracle Data Access Components (ODAC). You must install both the 32-bit ODAC drivers for the report writer, and the 64-bit ODAC drivers for EFT to work with Oracle.
- EFT supports the following Oracle versions:
  - Oracle Database 19c
- A good [database maintenance plan](#) is important to keeping space requirements to a minimum (aging/archiving/warehousing/truncating old data).
- For better database performance, follow the standard SQL/Oracle tuning guidelines in their respective documentation. See also [Purging Data from the Database](#).
- For ARM upgrades, Microsoft .NET Framework 4.0

## AS2 Module Requirements

- 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.
- Refer to [Installing and Activating the AS2 Module](#) for detailed prerequisites.

# Web Transfer Client (WTC) and Workspaces Requirements

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

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

## Advanced Authentication Modes Module Requirements

- To generate PCI DSS reports, you will also need the [Auditing and Reporting](#) module.
- For [Common Access Card authentication](#):
  - LDAP server
  - CAC smart card reader

- EFT v8.x does not support UPLOADS from [CAC-authenticated users](#) when using Chrome or Edge browsers. Firefox (and possibly other browsers) will work.
- For [RADIUS](#) or [RSA authentication](#):
  - RADIUS server
- For [SAML \(Web SSO\) authentication](#):
  - Identity provider (for example, [SafeNet](#), [Salesforce](#), [Shibboleth](#))

## Regulatory Compliance Module (RCM) Requirements

- To generate PCI DSS and GDPR reports, you will also need the [Auditing and Reporting](#) module.

## EFT Outlook Add-In Requirements

- The EFT Outlook Add-In is supported on Microsoft 365, Office 2016, Office 2019, with the latest service packs (as of this release).
- Microsoft .NET Framework 4.0
- Globalscape Support no longer tests the EFT Outlook Add-In with older versions, therefore it is not a supported configuration; however, some customers are still using those versions

## DMZ Gateway<sup>®</sup> Requirements

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

## Advanced Workflow Module Requirements

- Advanced Workflows v10 requires Microsoft .NET Framework 4.0

## Remote Agent Module (RAM) Requirements

- HTTP/HTTPS module
- SSL must be enabled and available on port 443
- Visual C++ and Redistributable for Visual Studio (for installation).
- EFT server must be registered
- Operating systems supported: Windows Server 2019, Windows Server 2016, Windows 10/ 11.
- After installation, the computer may require a reboot.

## Mobile Transfer Client (MTC) System Requirements

MTC is supported on:

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

## Content Integrity Control Action Requirements

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

- Clearswift (DLP) version 5\_5\_202211301821
- MyDLP Community Edition Server version 2.2.32-1
- Symantec DLP version 14.5.0.24028
- Kaspersky version 5.5

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

# EFT Specifications

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

## See also:

- [Safe Operating Limits for EFT](#)
- [EFT and AWE Encryption Algorithms](#)
- [System Requirements](#)

| Item   | Description   |
|--|---|
| <a href="#">PCI DSS</a>                        | EFT facilitates compliance with PCI DSS version 3.x.  |
| <a href="#">AS2 module</a>                     | EFT uses /n software's EDI Integrator library components, which are in the core of an application called RSSBus. RSSBus is Drummond Certified and in compliance with RFC4130. (EFT itself is not Drummond certified.) The maximum inbound file size for AS2 transfers is 20GB; there is no limit on outbound file size. |
| Advanced Workflow Engine (AWE) version         | EFT v8 uses <a href="#">Automate Desktop v10.7.100 Build 4</a> Task Builder and actions   |
| <a href="#">ICAP/Content Integrity Control</a> | <ul style="list-style-type: none"> <li>• EFT supports RFC3507, sections 3.2 and 4.9. EFT supports: draft-stecher-icap-subid-00 section 4.5 and 4.6.</li> <li>• Microsoft .NET Framework 4.0</li> </ul>  |
| EFT Outlook Add-In library                     | EFT v8.0.6 and later use Apache log4net v2.0.12   |
| RSA library                                    | EFT 8.1 and later use RSA® Authentication Agent API 8.6   |

| Item  | Description                                     |
|-------|---|
| RegEx | EFT uses the regular expression engine in .NET. |

## Safe Operating Limits

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

## EFT System Architecture

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

Refer to the [EFT System Architecture Guide](#) in the Knowledgebase for descriptions and illustrations of the various architectures available.

Talk to your account manager or the Globalscape [Professional Services team](#) to design a custom architecture.

# Installing EFT

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

Before you run the installer, review the [System Requirements](#), [EFT Specifications](#), and the Knowledgebase article, [Configuration and Best Practices](#).

- [Installation Logging](#)
- [Installing the Server, Interface, and Modules](#)
- [Active-Active HA Cluster—Installing or Upgrading the Server](#)
- [Active-Passive Failover Clustering--Installing or Upgrading](#)
- [Silent Command-Line Installation](#)

## 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.

# Installing EFT, Administration Interface, and Modules

The EFT installer is used to install EFT and its modules, except for [DMZ Gateway](#).

## Important Pre-Installation Information:

- **Before installing the software**, refer to [System Requirements](#), and read the entire installation procedure below. Also review "Important information" in [Installing the Advanced Workflow Module](#).
- After you have installed the system on a test computer and are now ready to move it to a production environment, refer to [Backing Up or Restoring Server Configuration](#) if you want to keep the test environment's Server, Site, and user configuration settings. Otherwise, perform a clean install as usual on the production system.
- **If you are installing in a cluster configuration**, refer to [Installing or Upgrading the Server in a Cluster](#).

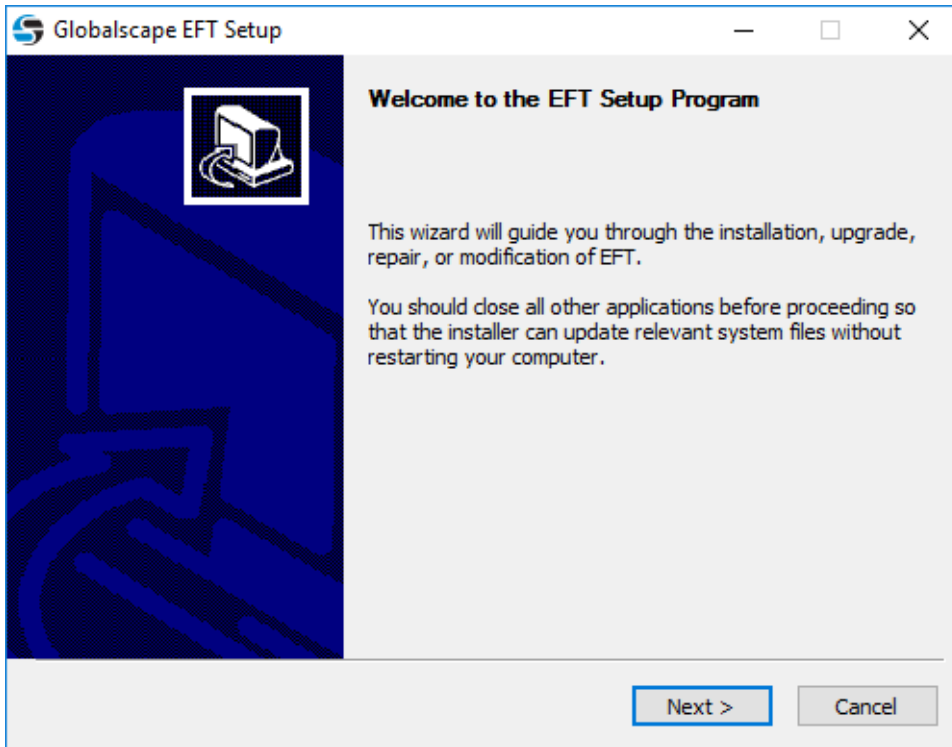
- **If you are connecting to an existing database**, ensure the database is installed and configured before starting the EFT installer. The installer will attempt to connect to the database. Or you can skip ARM installation and rerun the installer later in **Modify** mode.
- **If you are using an Oracle database**, ensure the [ODAC client](#) suitable for your database version is installed. (Refer to [System Requirements](#).) For details of installing SQL Server, refer to the [SQL Server Install pages](#) on [technet.microsoft.com](http://technet.microsoft.com).
- The EFT installer includes the ARM database installation and upgrade files. If you want to install or upgrade the database later, refer to [Installing and Configuring the Auditing and Reporting Module](#), [Upgrading the EFT Database](#), [Upgrading Large Databases](#), and [EFT Database Utility](#).
- The EFT installer does not support Unicode characters. Refer to [Unicode Exceptions](#) for details.

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

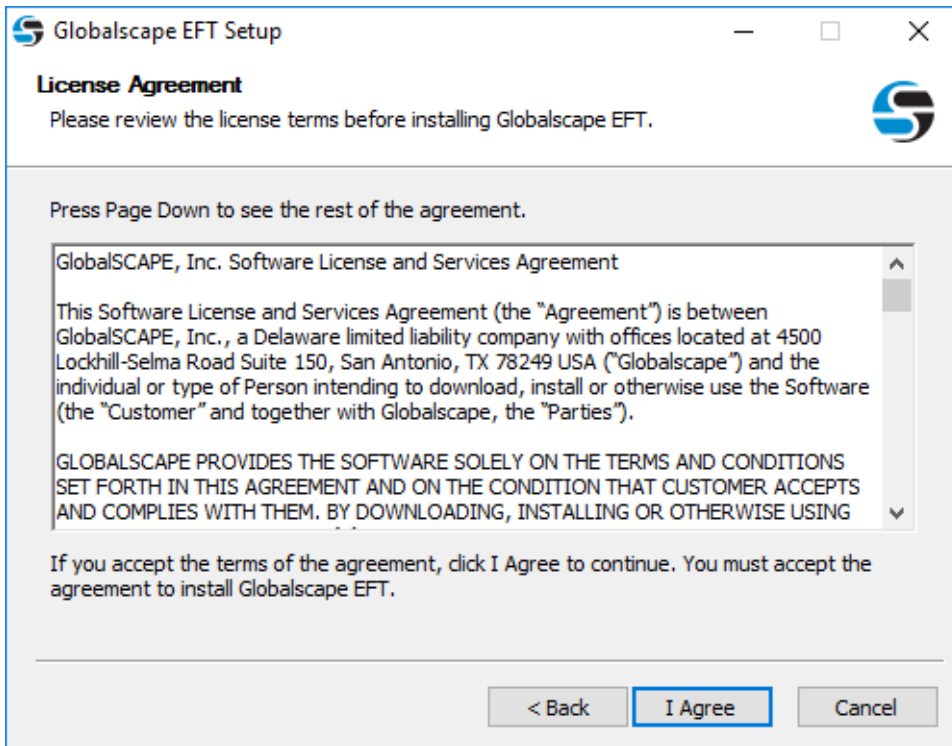
- OS compatibility
- Is the user an administrator?
- DMZ Gateway is **not** installed on this server?
- Correct .NET version installed?
- MSI 4.5 installed?
- MSMQ installed? ([HA installations](#) only)

**To install EFT, administration interface, and all modules except for [DMZ Gateway](#)**

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

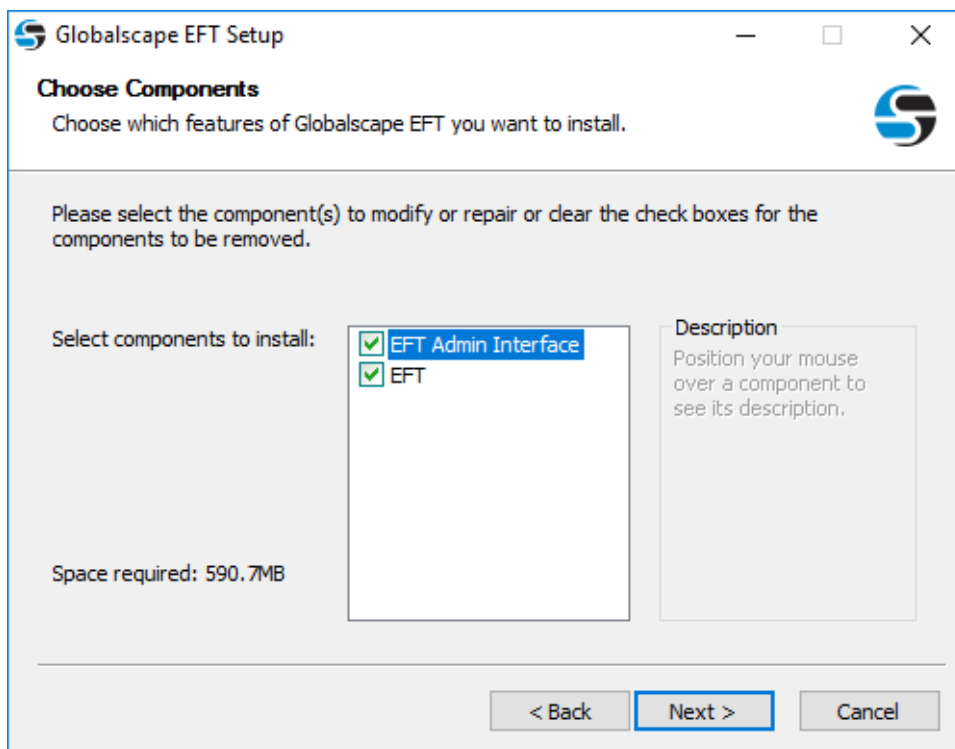


3. Read the **Welcome** page, and then click **Next**. The **License Agreement** page appears.



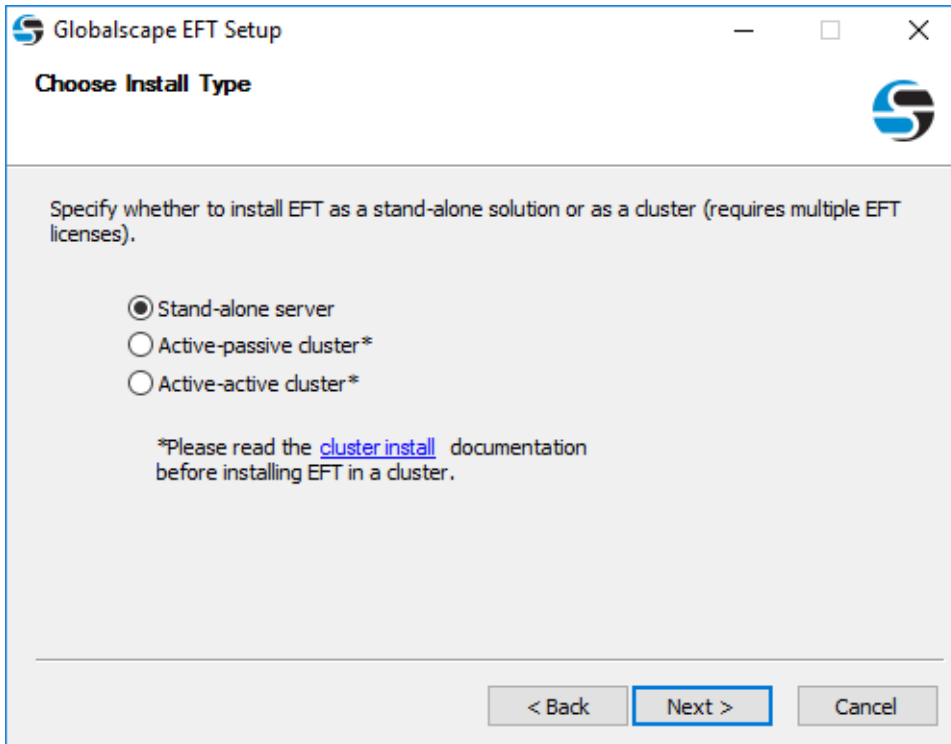
4. Read the license agreement, and then click **I agree** to accept it. Clicking **Cancel** aborts the installation.
  - If you are upgrading or reinstalling, the version detected page appears. Refer to [Upgrading the Software](#) for the procedure.

The **Choose Components** page appears.



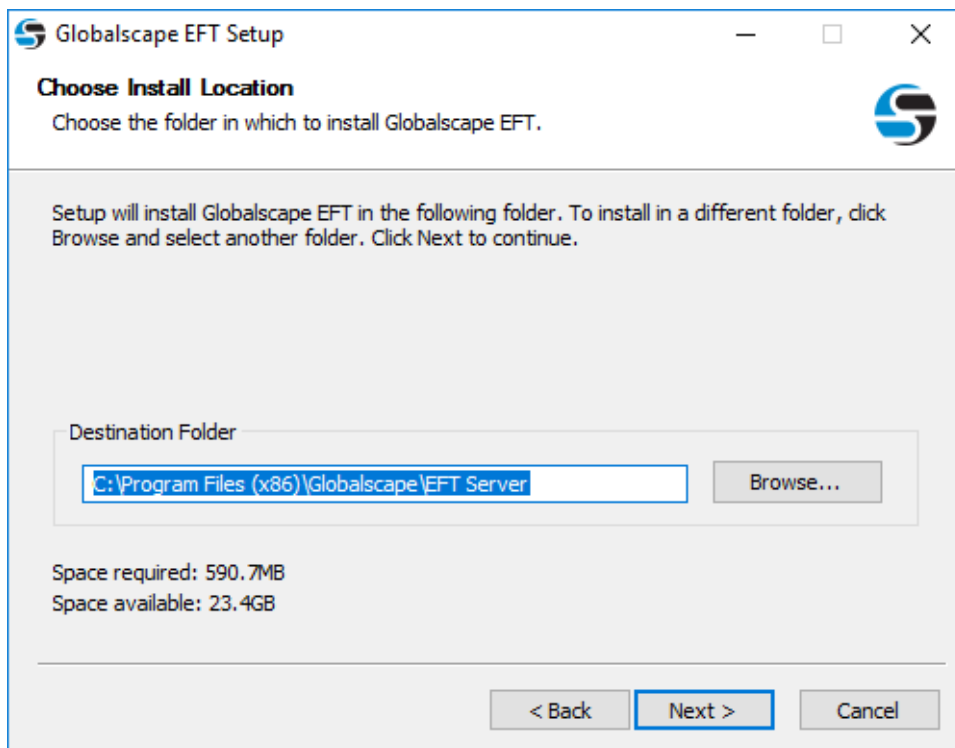
When you install EFT, the **EFT administrator Interface** check box must also be selected. After you have installed EFT and the administration interface on one computer, you can install the administration interface on other computers for remote administration (optional). (To install the administration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

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

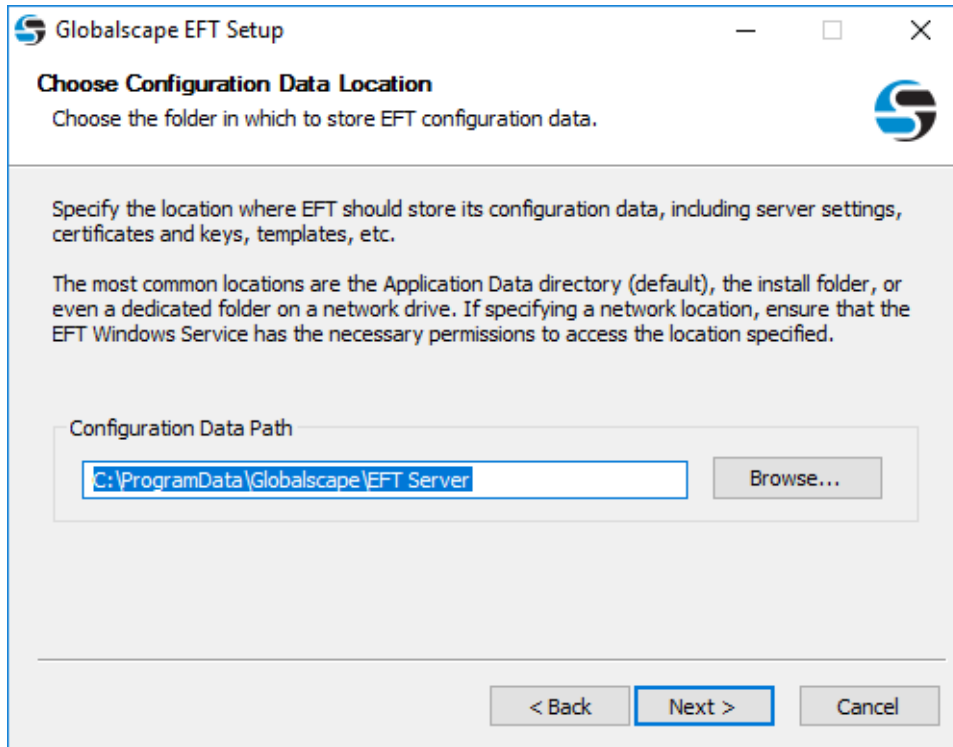


6. Specify the installation type, and then click **Next**.
  - Single server is the default installation type.
  - To install EFT as part of a failover cluster, review the cluster documentation, and then click **Part of a failover cluster**. A message appears cautioning that it is important to read and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

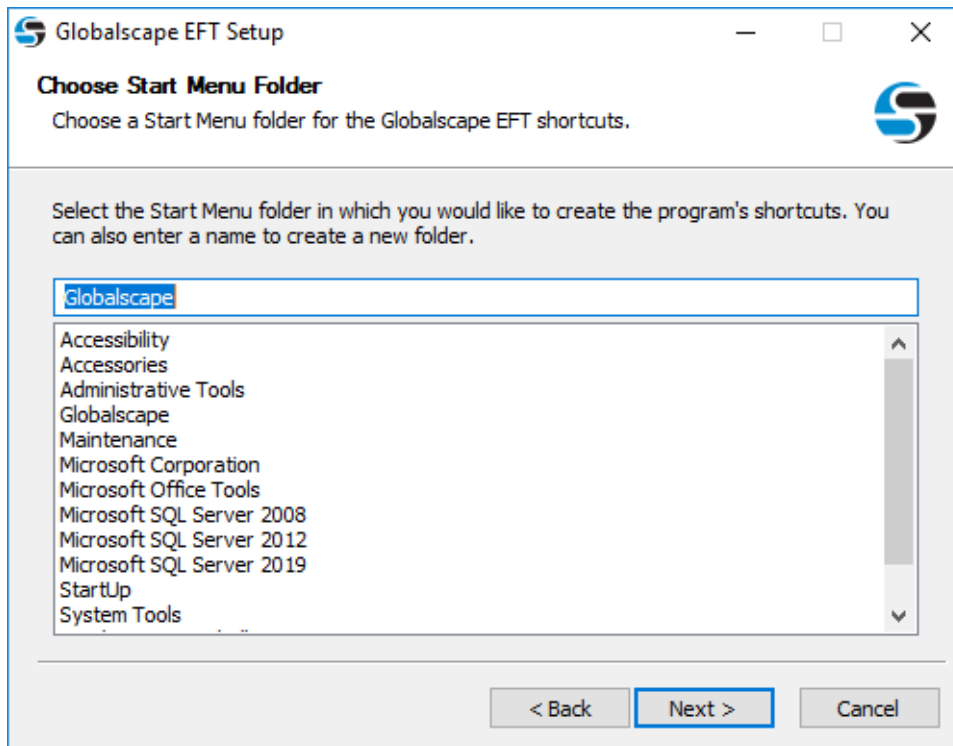
The **Choose Install Location** page appears.



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



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



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

**EFT Administrator Account Configuration.**  
Specify the EFT administrator username and password.

Please create a user name and password for the EFT administrator account.

The user name and password are case sensitive.

Administrator Username:

Password:

Confirm Password:

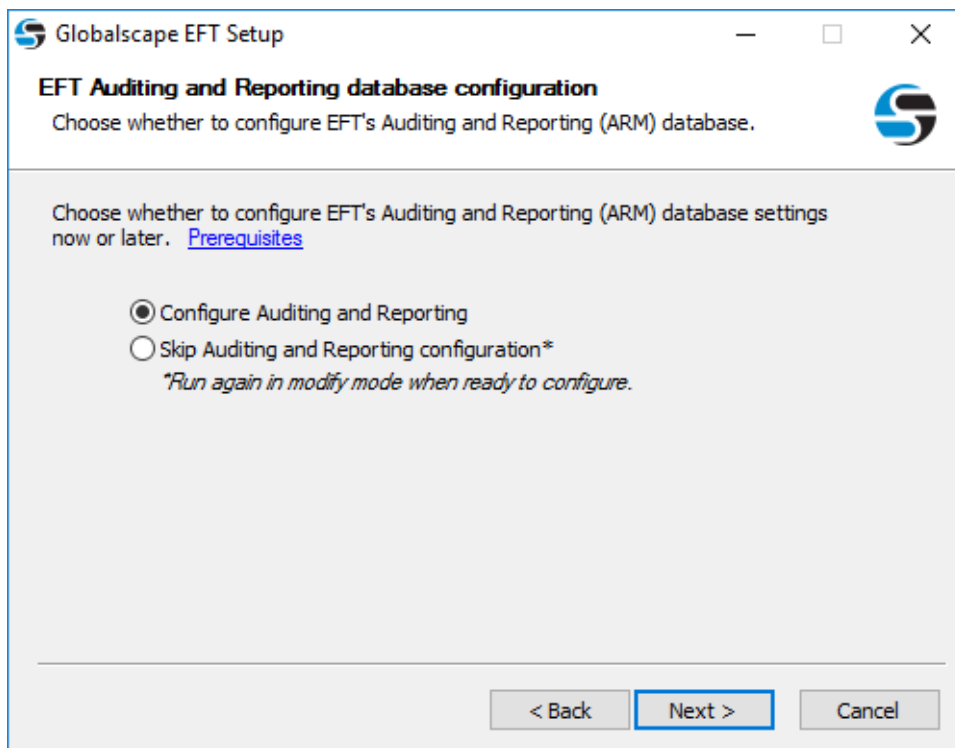
Note: After installation is complete you will be able to configure Active Directory accounts for administration (if preferred over EFT managed accounts).

< Back   Next >   Cancel

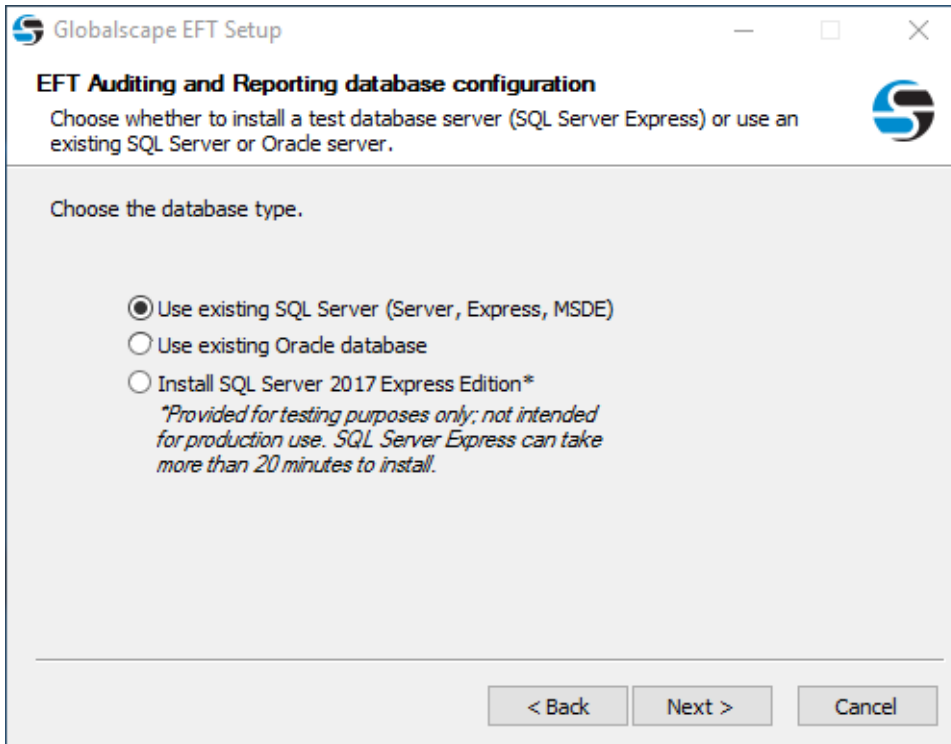
12. Create a user name and password for the administrator account for connecting to EFT from the administration interface. Both the username and password are case sensitive. The installer does not support [Unicode characters](#) in the username or password.

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

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



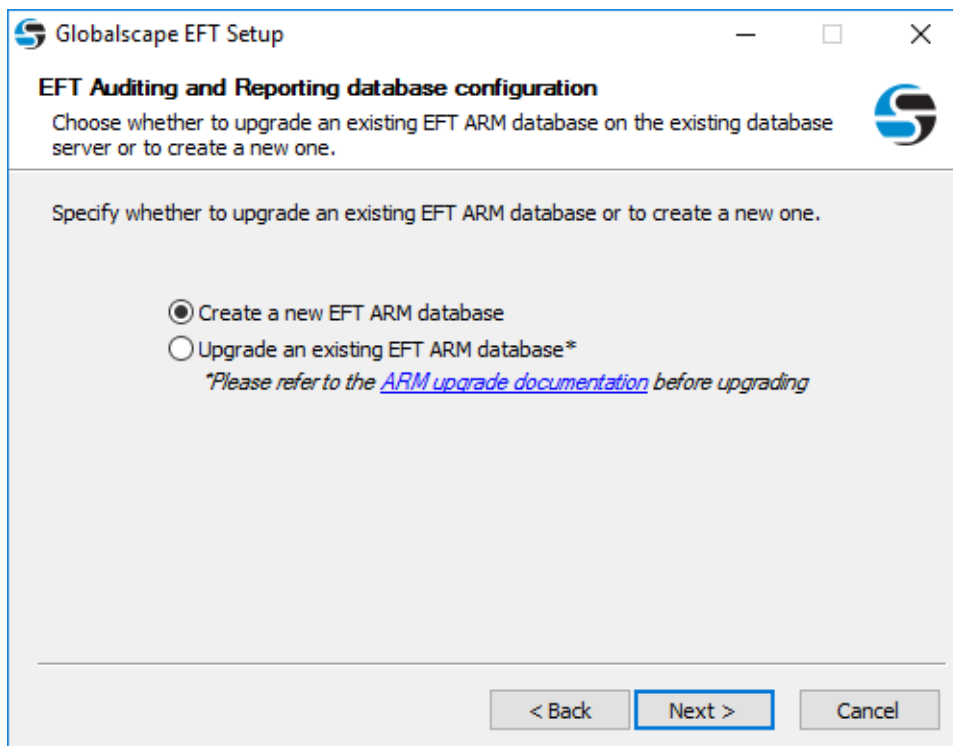
- If you want to configure auditing and reporting, click **Next**.
  - If you do not want to configure auditing and reporting, click **Skip auditing and reporting configuration**, and then click **Next** to skip the database configuration pages. You can still configure the database later, if you want. (Skip to step [18](#).)
  - If you want to manually create the database later, click **Skip auditing and reporting configuration**, and then refer to [Manually Creating the ARM Database in SQL Server](#) or [Manually Creating the ARM Database in Oracle](#) when you're ready to create the database. (Skip to step [18](#).)
14. Specify the type of database, SQL Server or Oracle, that EFT is to use. You will need the connection information available to point EFT to the database. If you already have a database to use, then you do not need to install SQL Server Express. (If you are using the "no db" installer, you will not see the "Install SQL Server" option.)



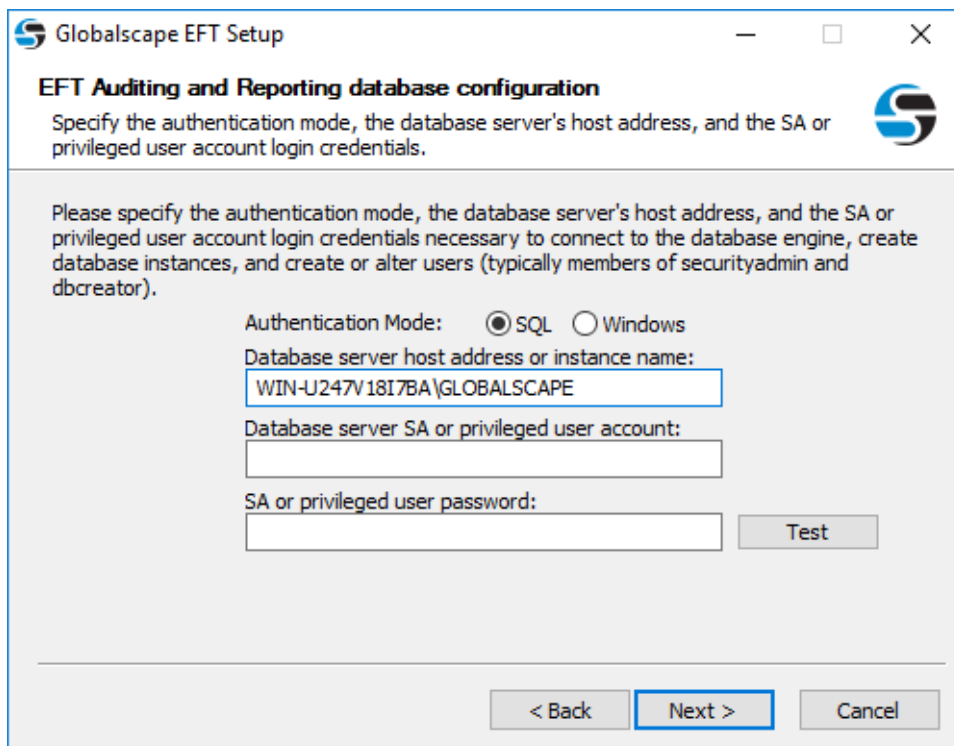
- **Install SQL Server Express**

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

- **Use existing SQL Server:**



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



- b. Specify **Windows** or **SQL** Authentication. (**Windows** mode allows you to connect through a Microsoft Windows NT or Windows 2000 user account. **SQL** allows you to connect using either Windows Authentication or SQL Server Authentication.)
  - c. Specify the host address or instance name.
  - d. Specify the database server SA or privileged user account name (for example, sa).
  - e. Specify the database server SA or privileged user account password
  - f. (Optional) Click **Next** or **Test** to test the connection to the database. If the test fails, click **Yes** to verify database connection details or **No** to continue without configuring the database.
- **Use existing Oracle database:**
    - a. Click **Create a new schema**. The configuration page appears.

The screenshot shows a Windows dialog box titled "Globalscape EFT Setup" with the subtitle "EFT Auditing and Reporting database configuration". The dialog contains the following text and fields:

Specify the Oracle database server's host address, database name, and database administrator credentials.

Please specify the database server's host address, database name, and database administrator credentials for creating the ARM schema.

Database host address (address:port)

EFT ARM database name:

User Name:

Password:

Test

< Back   Next >   Cancel

- b. Specify the database host address and the EFT-specific schema name and database administrator credentials, and then click **Test** or **Next** to test the connection to the database. (If you have installed Oracle Database Express Edition (XE) for testing/demo purposes, the instance name is XE and the User Name is SYSTEM.)
    - If the test fails, click **Back** to verify the configuration or click **Next** and then **Next** again to open the [Oracle Technology Network download page](#) and download "Oracle Data Access Components for Windows" driver, if necessary.
15. After the test is successful, click **Next**. The ARM schema owner credentials page appears.

Globalscape EFT Setup

**EFT Auditing and Reporting database configuration**

Specify the authentication mode, the database name, and the database owner credentials.

Specify the database owner credentials and authentication mode: Windows (logged on user account) or SQL. If SQL account exists, it will be assigned as the database owner; if not, it will be created and assigned as owner.

Authentication Mode:  SQL  Windows

EFT ARM database name:  
EFTDB

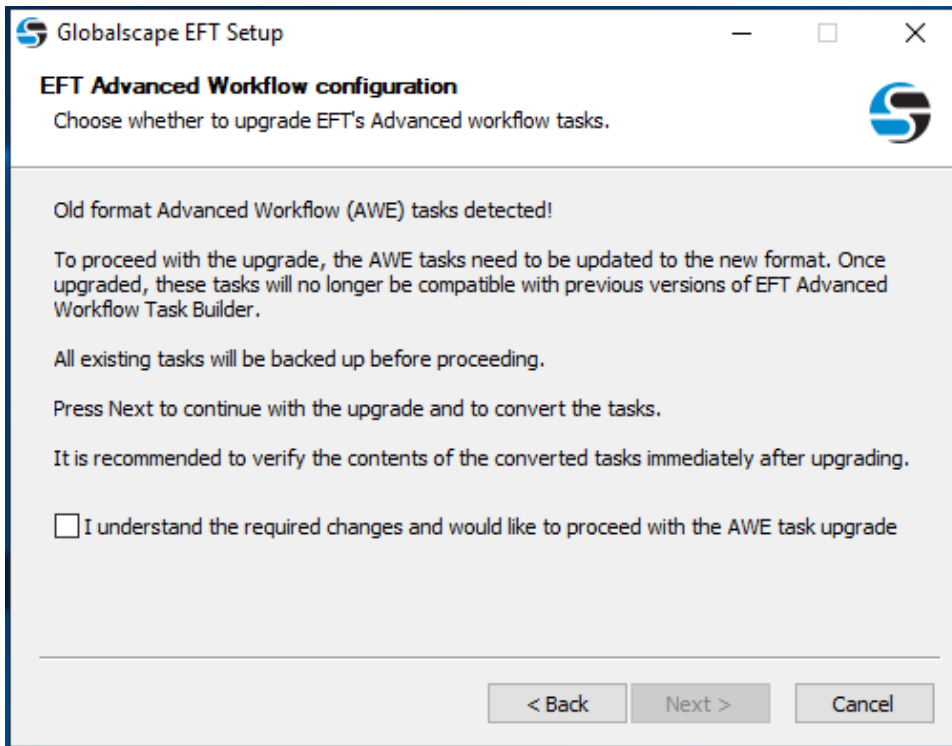
Database owner username:  
[ ]

Database owner password:  
[ ]

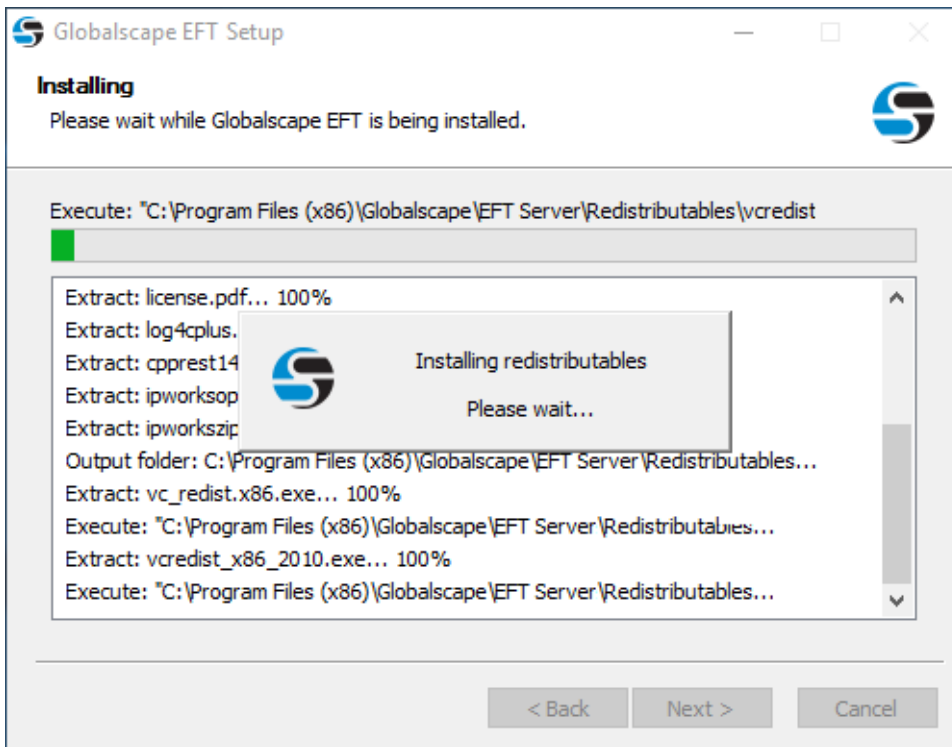
Confirm owner password:  
[ ]

< Back Next > Cancel

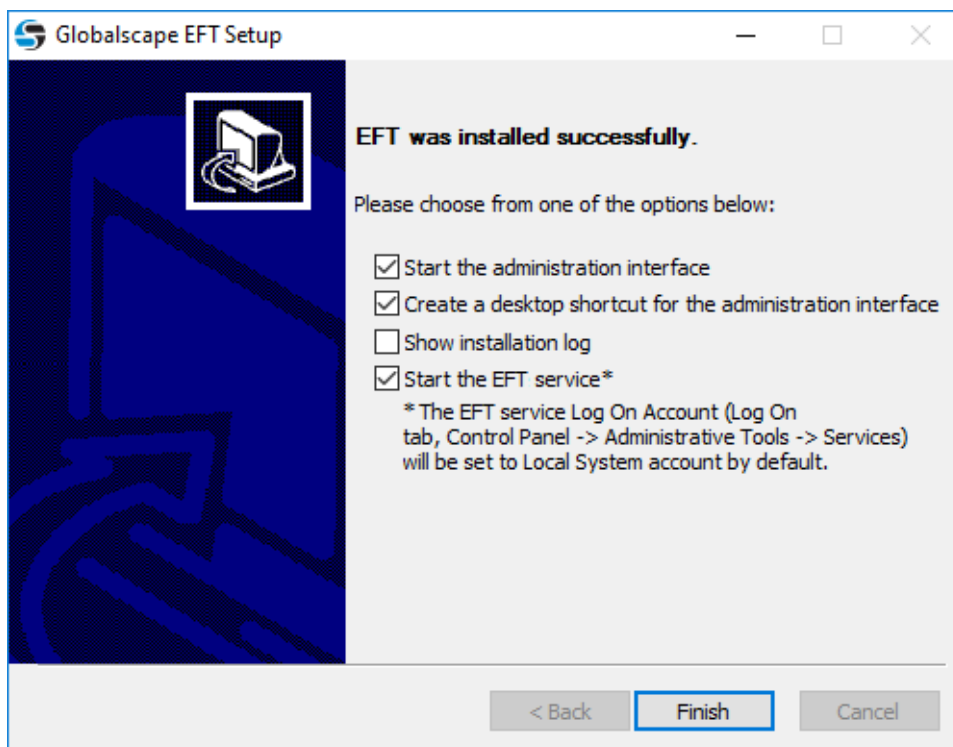
16. Specify or create the ARM schema owner credentials, then click **Next**. The installer creates the tables.
17. If this is not the first installation of EFT, the EFT Advanced Workflow configuration page appears.



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



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

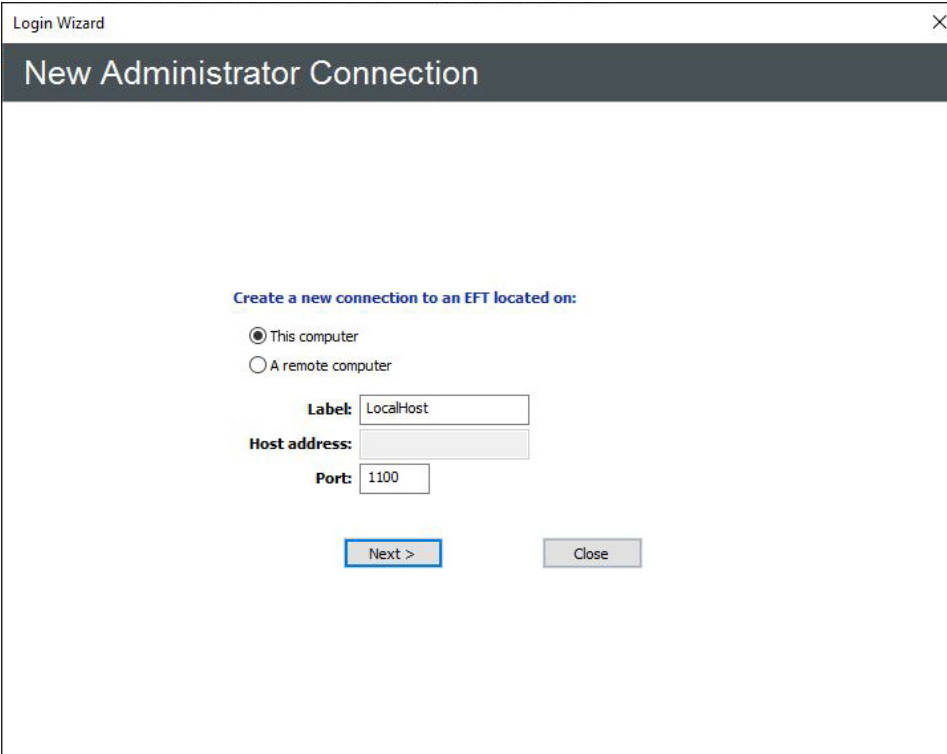


- **Start the administration interface** - If you do not want to open the interface, clear the check box. You can also open the interface from the **Start** menu.
- **Create a desktop shortcut** - An administration interface shortcut is created on the desktop by default. If you do not want to create a shortcut, clear the check box.
- **Show version history** - If you want to read the release notes, select the **Show Version History** check box. If you want to read it later, the file, **notes.txt**, is stored in the EFT installation directory.
- **Show installation log** - If you want to review the installation log now, select the check box. If you want to review it later, it is stored in a temporary folder, **C:\Program Files\GlobalSCAPE\EFT Server\Installer.log**.

- **Start the EFT Server Service** - Clear the check box if you do not want to start the Service yet. Select the check box if you want to start the service when you click **Finish**. The service is configured to start automatically when the computer starts. If you do not want the service to start automatically, you will have to configure it in Windows to start manually. The EFT service Log On Account is set to "Local System account."

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

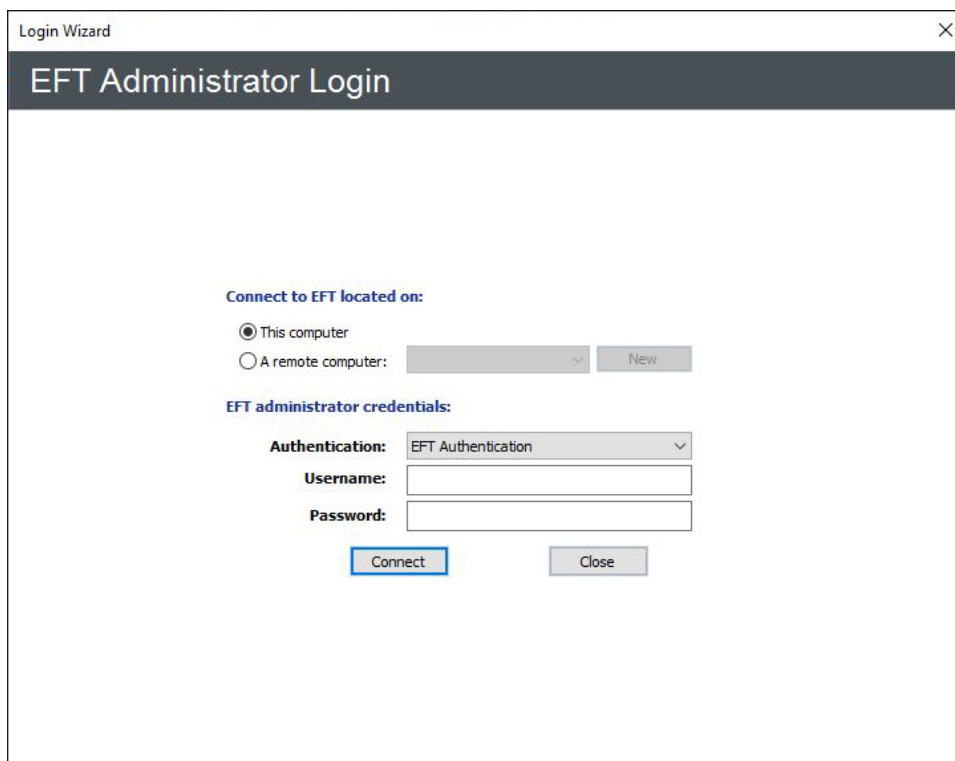
19. Click **Finish**. If the administration interface check box was selected and the EFT service was started, the **Login Wizard** appears.



The screenshot shows a window titled "Login Wizard" with a close button (X) in the top right corner. Below the title bar is a dark header with the text "New Administrator Connection". The main content area contains the following elements:

- A blue heading: "Create a new connection to an EFT located on:"
- Two radio buttons:
  - This computer
  - A remote computer
- Three input fields:
  - Label:** LocalHost
  - Host address:** (empty)
  - Port:** 1100
- Two buttons at the bottom:
  - Next >** (highlighted with a blue border)
  - Close**

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



The screenshot shows a window titled "Login Wizard" with a close button (X) in the top right corner. The main title bar reads "EFT Administrator Login". Below the title bar, the text "Connect to EFT located on:" is displayed. There are two radio button options: "This computer" (which is selected) and "A remote computer:". To the right of "A remote computer:" is a text input field and a "New" button. Below this, the text "EFT administrator credentials:" is displayed. There are three fields: "Authentication:" with a dropdown menu showing "EFT Authentication", "Username:" with a text input field, and "Password:" with a text input field. At the bottom, there are two buttons: "Connect" and "Close".

21. Click in the **Authentication** box and specify the type of authentication to use for this login. Future connections will default to the authentication type that you specify during this initial login, but you can choose a different type. Authentication types include:
- **EFT Authentication** - Choose this option to log in with an EFT-specified administrator account, such as the one you created during installation.
  - **Integrated Windows Authentication** - Choose this option to log in with an Active Directory or local Windows account.
  - **Windows NET logon** - Choose this option to log in with a local Windows account.

22. In the **Username** and **Password** boxes, provide the login credentials that you created during installation, and then click **Connect**. The **Welcome** page appears. Since you have not yet activated the software, the "Free Trial" reminders appear. After you activate, you will not see the reminder prompt.

**Next Steps:**

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

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

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

## Installing the Advanced Workflow Module

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

**NOTE:** Do not use your Automate license key with EFT, as the Advanced Workflow Module (AWM) license is managed by the EFT licensing server. Having an Automate license does not grant a license in EFT to unlock the Advanced Workflow Module (AWM) in EFT.

The Advanced Workflow module is registered in the EFT administration interface. Please refer [Activating the Software](#) for details.

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

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

See also [Upgrade HA Nodes with Zero Downtime](#).

## Active-Passive Failover Clustering-- Installing or Upgrading

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

# After You Are Done

Congratulations! EFT is now installed.

Next steps:

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

## Configuration and Security Best Practices

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

# Creating and Configuring an EFT Server

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

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

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

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

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

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

- If you are allowing remote administration of EFT and you are [using SSL](#), you need to know the SSL settings and have access to the SSL keys and certificates.
- If you are restricting remote administration to specific IP addresses, you need to know the IP addresses and ports.

- If you are using DMZ Gateway, install and configure DMZ Gateway (on a different computer). The installation and configuration of DMZ Gateway is not *required* before creating Servers and Sites, but the Site setup wizard asks for the DMZ Gateway information. Alternatively, you can configure DMZ Gateway after Site setup is complete, and then provide the DMZ Gateway connection information in EFT's administration interface.

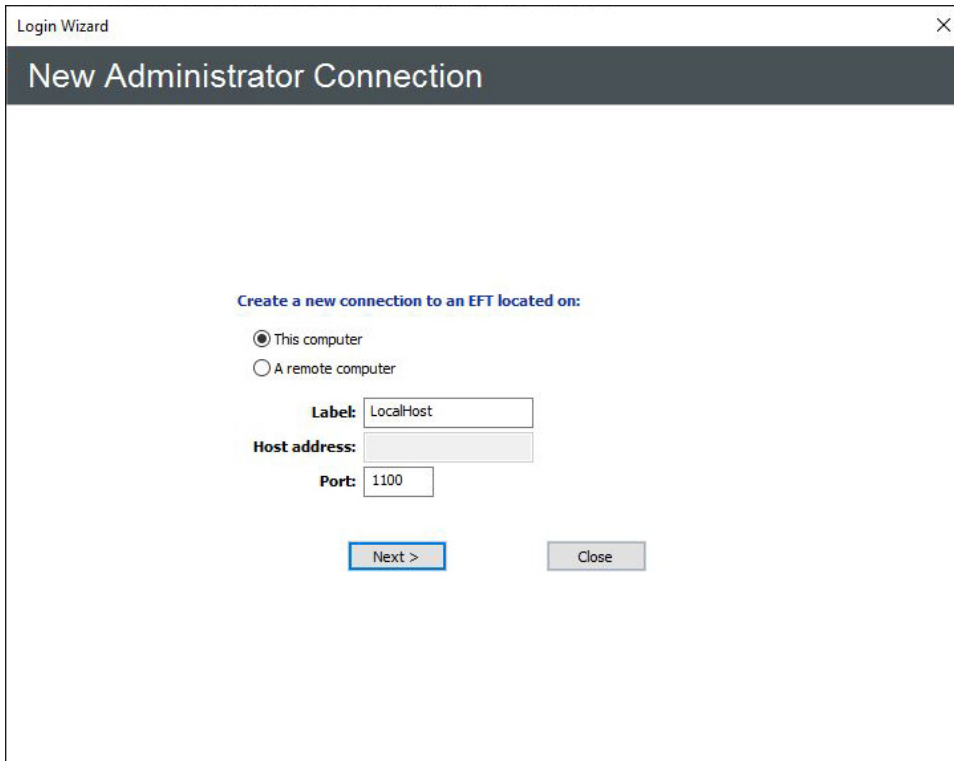
If you are configuring your first EFT Server connection, refer to [Configure the First EFT Connection](#), below. If you are configuring a new, remote EFT connection, refer to [Creating a Remote Connection](#).

## Configure the First EFT Connection

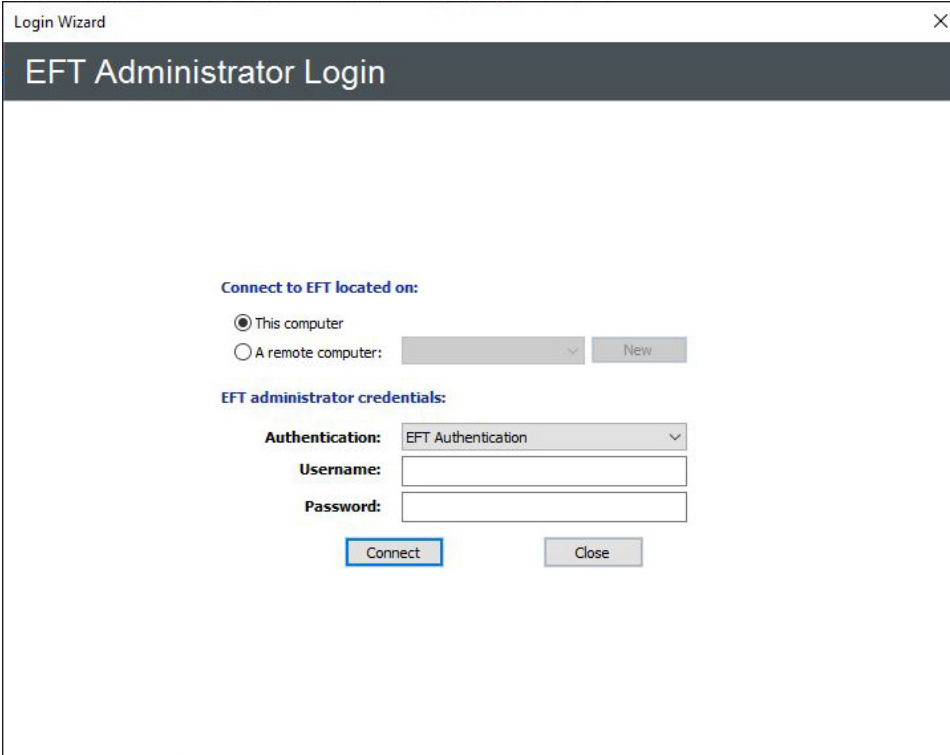
You must first configure the local connection before you can configure a remote location.

### To configure EFT on the local computer

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



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



The screenshot shows a window titled "Login Wizard" with a close button (X) in the top right corner. The main title of the window is "EFT Administrator Login". Below the title, there are two sections:

**Connect to EFT located on:**

- This computer
- A remote computer: [text box] [New]

**EFT administrator credentials:**

**Authentication:** [EFT Authentication] [v]

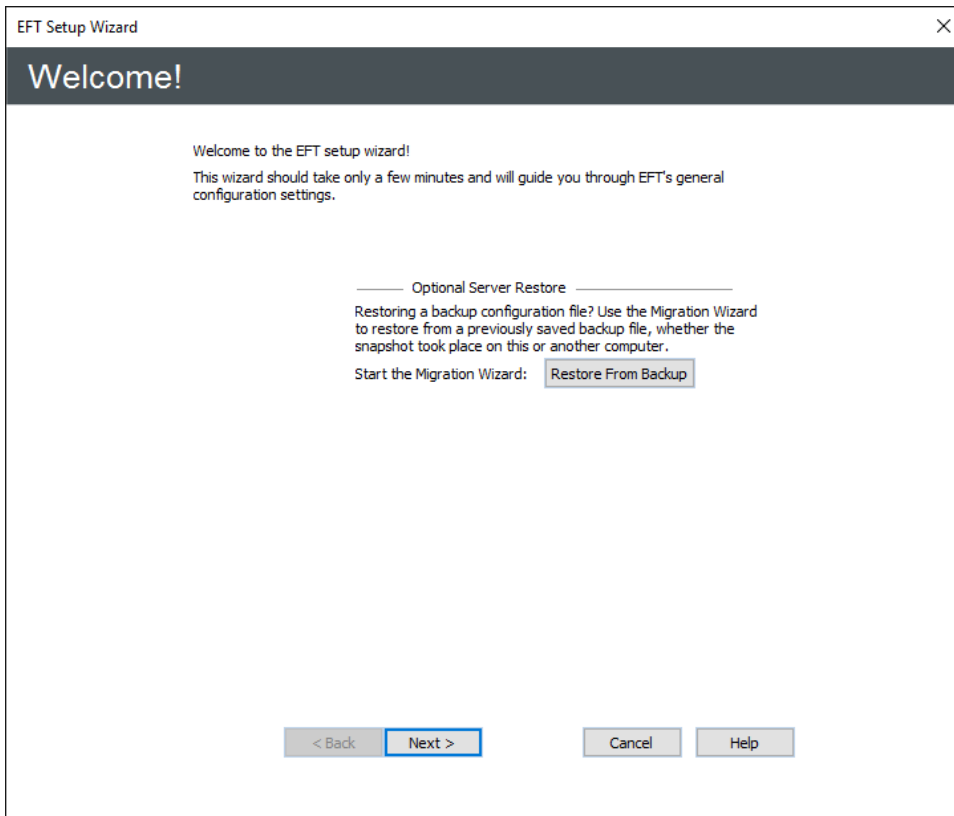
**Username:** [text box]

**Password:** [text box]

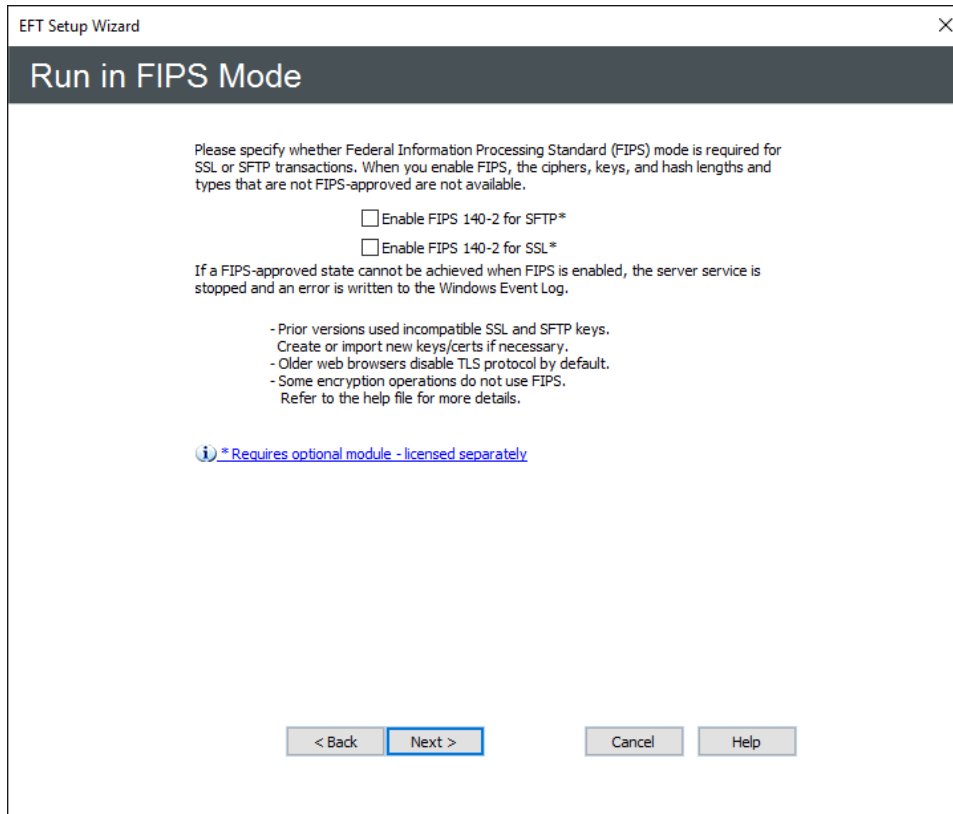
[Connect] [Close]

3. Click the **Authentication** box and specify the type of authentication to use for this login. Future connections will default to the authentication type that you specify during this initial login, but you can choose a different type. Authentication types include:
  - **EFT Authentication** - Choose this option to log in with an EFT-specified administrator account, such as the one you created during installation.
  - **Integrated Windows Authentication** - Choose this option to log in as the currently logged on user (Integrated Windows Authentication).
  - **Windows Authentication** - Choose this option to log in using a specific Windows account.
4. If you specified **EFT Server Authentication** or **Windows Authentication**, in the **Username** and **Password** boxes, provide the login credentials that you created during installation. The **Welcome** page appears. Because you have not yet activated the software, the "Free Trial" reminders appear. After you activate, you will not see this prompt.

5. Do one of the following:
  - If you are evaluating the software or just do not want to activate yet, click **Start Trial**, then follow the procedures in [Creating and Configuring an EFT Server](#).
  - If you have purchased a license, click **Activate Now**, then follow the procedures for [activating the software](#).
6. Click **Next**. The **Server Setup** wizard **Welcome** page appears.



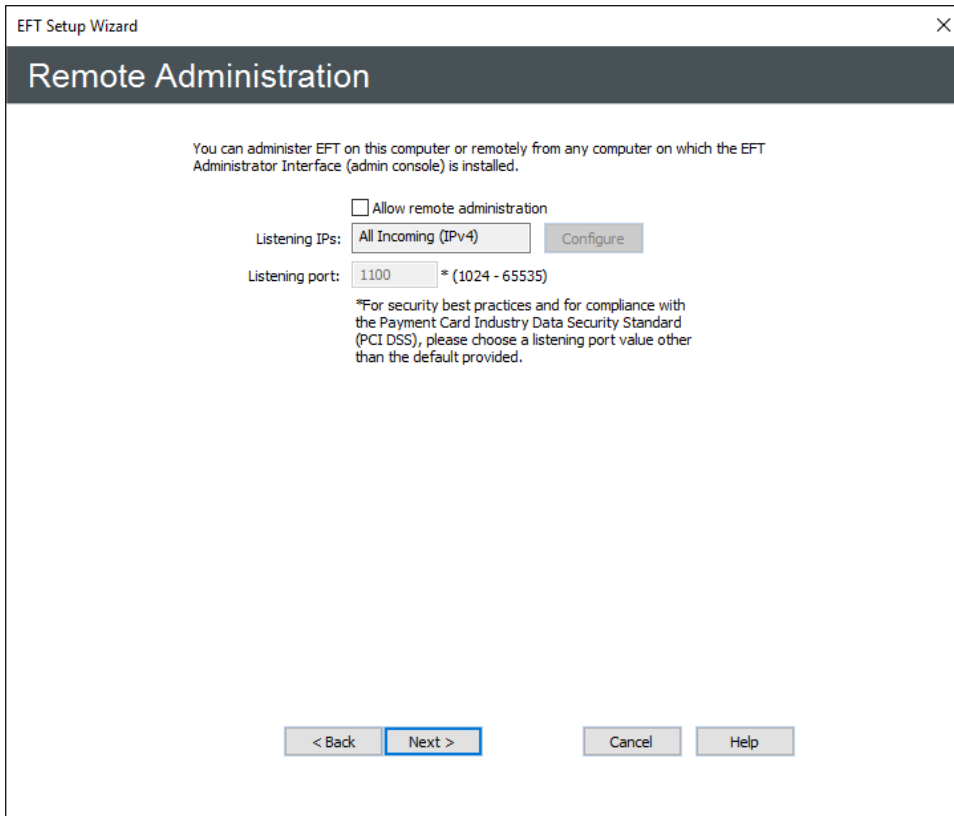
- If you are not restoring from a [backup](#), click **Next**.
  - If you are restoring from a backup, click **Restore from Backup**, then refer to [Backing Up or Restoring Server Configuration](#) for the procedure.
7. Click **Next**. The **FIPS Options** page appears.



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

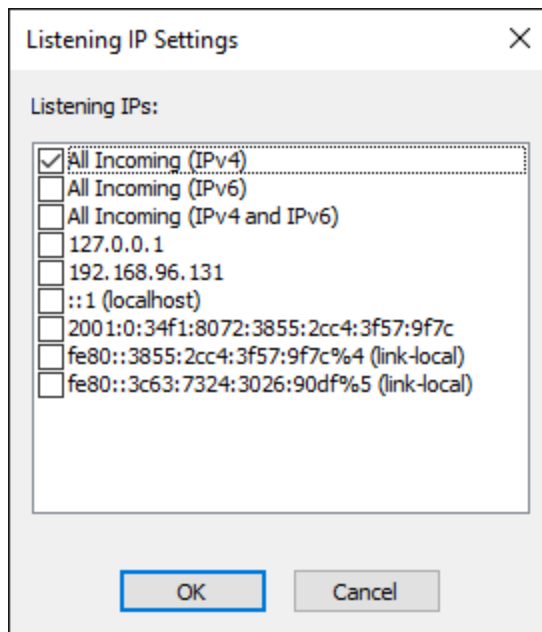
- To use FIPS for SFTP (SSH2), select the **Enable FIPS for SFTP** check box. To use FIPS for SSL, select the **Enable FIPS for SSL** check box.
- A confirmation prompt appears when you select either check box. When you enable FIPS, the EFT service must be restarted. Click **OK** to continue with FIPS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

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

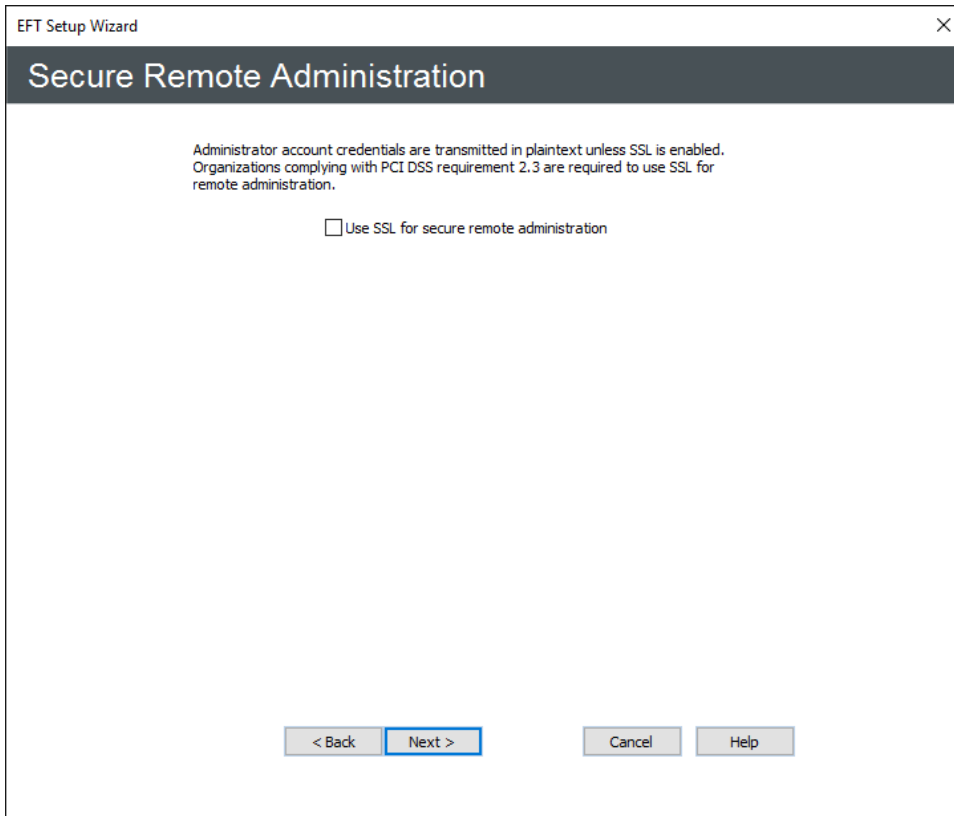


- If you do not want to allow [remote administration](#), clear the **Allow remote administration** check box.
- If you want to allow remote administration:
  - a. Select the **Allow remote administration** check box and specify the **Listening IPs**.
  - b. Click **Configure** to specify one or more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

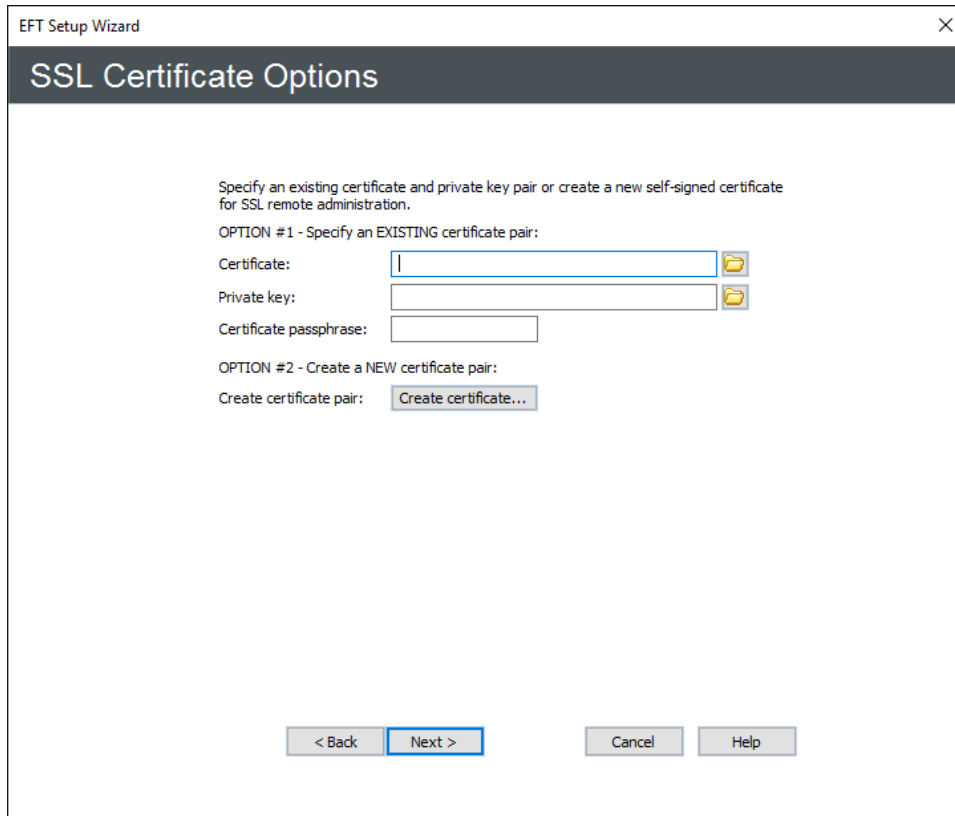
**Settings** dialog box appears.




- **All Incoming (IPv4)** is selected by default. Select the check boxes for addresses that you want to allow; clear the check boxes for the addresses that you do not want to allow, then click **OK**.
9. Specify the **Listening port**. (For security best practices and compliance with the PCI DSS, specify a port other than the default of 1100.)
  10. Click **Next**. If you chose remote administration, the **Secure Remote administration** page appears.



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



12. Do one of the following:

- In the **Certificate** and **Private Key** boxes, click the folder icon  to browse for the private key pair files.
- Click **Create certificate** to create one. Refer to [SSL Certificate-Based Login, Creating Certificates](#) and [Importing a Certificate into the Trusted Certificate Database](#) for information regarding certificates.

13. Click **Next**. The **Auditing and Reporting** page appears.

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

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

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

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

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

The screenshot shows a window titled "EFT Setup Wizard" with a close button in the top right corner. The main heading is "SMTP Server Settings". Below the heading, there is a sub-heading: "Specify your SMTP server settings for outbound e-mail notifications." The form contains the following fields and options:

- "From e-mail address\*:" followed by a text input field. A note below it states: "\*This is the address that will appear in the 'From:' field of EFT generated e-mails. e.g. noreply@host.com, eft@host.com."
- "SMTP host address:" followed by a text input field and "Port:" followed by a text input field containing the value "25".
- A checkbox labeled "Use SMTP server authentication:".
- "Username:" followed by a text input field.
- "Password:" followed by a text input field.
- A checkbox labeled "Use Implicit TLS".
- A "Send Test Email" button.
- Navigation buttons at the bottom: "< Back", "Next >", "Cancel", and "Help".

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

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

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

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

20. Click **Send Test Email** to ensure the credentials are correct.
21. Click **Next**. Server Setup is complete.

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

22. 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.
23. If you chose **Run the Site Setup wizard now**, the Site Setup wizard **Welcome** page appears.
24. Next, refer to [Creating a Site](#) for the procedure for configuring the first Site.

## Activating the Software (Licensing EFT and Modules)

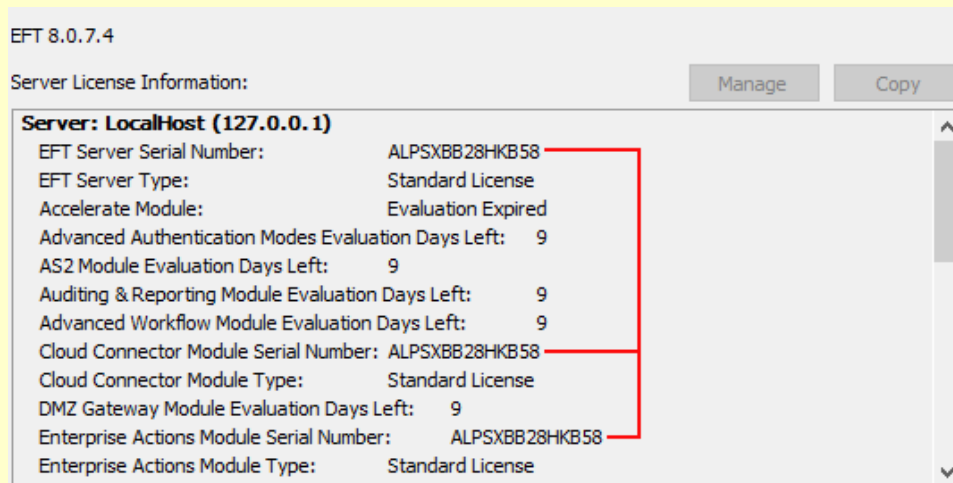
The EFT server with FTP is free, but you should still register your EFT serial number in case you need support. EFT on-premises licenses are available as a perpetual license (register once and never have to register again, except in some upgrade instances), or as a monthly or yearly subscription.

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

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

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

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



- If you run into an issue where your EFT Server license will not work, please contact support. Do not enter any other serial numbers until EFT has been registered.
- If you register a module without first registering EFT, then our registration process will not work properly and you might have troubles should you need support.
- Registration of EFT with older EFT Server Enterprise or Express serial numbers are supported; this will unlock certain features similar to an upgrade scenario.
- Manual registration of EFT with older EFT Server Enterprise or Express serial numbers is supported, however, we recommend you work with our support team.

- EFT 8.0.7 and later do not support DMZ Gateway single site registration via manual registration.
- Do not use your Automate license key with EFT, as this is managed by EFT's licensing. Having an Automate license does not automatically grant a license in EFT to unlock the Advanced Workflow Module (AWM) in EFT.

## Registering EFT and the Modules

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

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

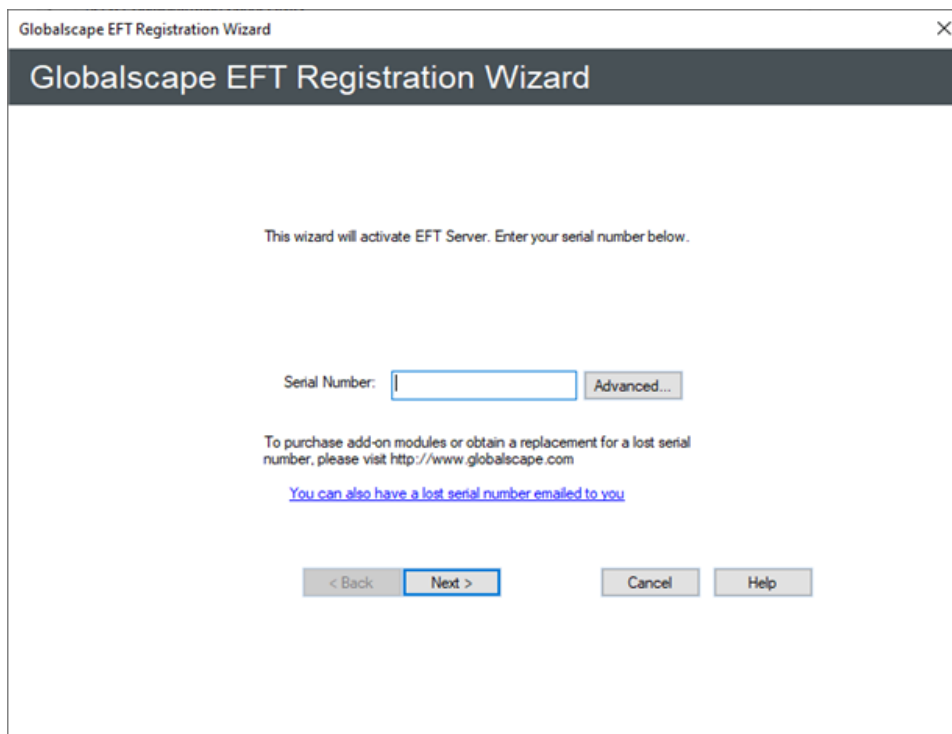
**To activate online**, you must be connected to the Internet, and activation must be performed through the administration interface on the EFT computer. You cannot activate through a remote installation of the administration interface.

Refer to [If you do not have Internet access on the EFT computer](#) for manual registration without the Internet.

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

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

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



2. In the **Serial Number** box, provide your serial number, and then click **Next**.  
See [below](#) for Advanced Registration Options, if needed. The Advanced Registration Options are not required for successful registration, but is for specific use cases with manual registration, or to determine if the registration server is returning a registration limit error. (A DMZ Gateway multi-Site license requires manual registration.)
3. You should receive a message confirming online activation. Click **OK**. Activation is complete. (If registration fails, try entering your serial number again.)
4. The **Help > About** dialog box displays the status of the activation, such as number of licenses on certain modules, and whether it is a standard or subscription license, and renewal date.

## Subscription Licenses:

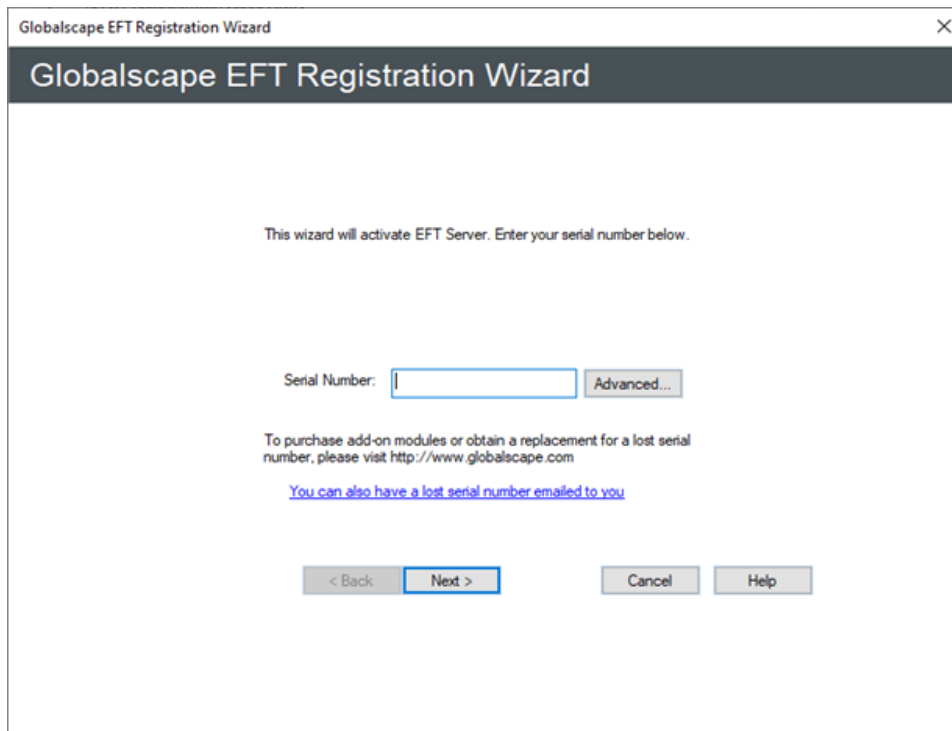
**IMPORTANT:** Internet access is a pre-requisite to complete activation and renewal of a subscription license. EFT reaches out to the server at **dbregistration.globalscape.com** on port 80 to send the registration request, and receive the registration response back. If EFT cannot connect directly, it will attempt to connect via each DMZ Gateway defined (as a proxy) in turn. If that still fails, please contact Support. There is no manual process for **subscription** licenses at this time.

- A subscription license key can be used to activate EFT and modules.
- Click **Help > Activate** [product name], and follow the prompts to active your license (s).
- The **Help > About** dialog box displays the subscription license type and the subscription term, which is based on the term dates stated in your invoice.
- Upon the renewal date, EFT will attempt to re-activate the license and, therefore, must have internet access at that time.
  - If there are additional months/years remaining in your term, EFT will successfully renew and start its countdown to the next renewal date.
  - If your subscription has run out or if EFT encounters any other problem during renewal, EFT will enter a grace period, also indicated in **Help > About**.
- During the grace period, EFT will attempt to renew the subscription every hour, if possible, for about a week, before it finally gives up or succeeds. During this period, EFT will display warnings upon administrator login, and will log an event to the Windows Event Log. This grace period affords you the time to contact sales and renew if your subscription, if desired.
  - If it succeeds, then all is well and the new renewal date is shown in the **Help > About** dialog box.
  - If it fails, then EFT will enter its pre-activation state, where all modules become disabled and all protocol activity will cease.

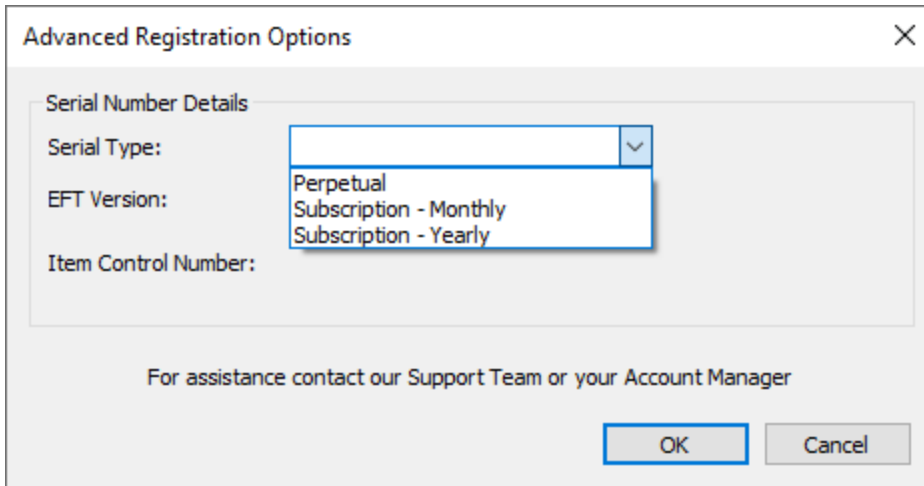
The Advanced EFT Registration options allow EFT administrators to provide more details on a registration request so that they can obtain proper registration status or correct manual registration details. When the Advanced Registration Options is configured and submitted to the registration server, EFT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

### To register a subscription license

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

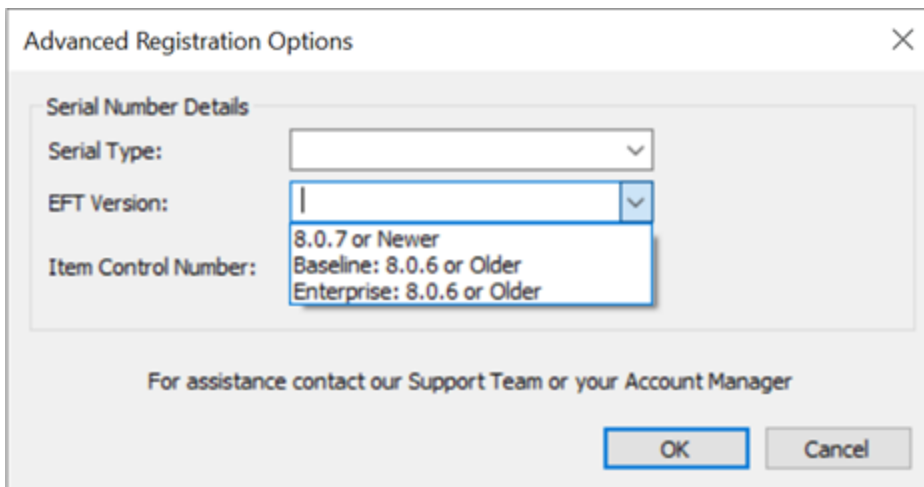


3. Next to the **Serial Number** box, click **Advanced**. The **Advanced Registration Options** dialog box configures specific serial number details that are then sent to the registration server.
4. In the **Serial Type** box, click the drop-down list and click the type of serial number: **Perpetual**,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



5. In the **EFT Version** box, click the drop-down list and click the version number you are registering. (For example, **8.0.7 or Newer**, **Enterprise: 8.0.6 or Older**, **Express: 8.0.6 or Older**.) Select **8.0.7 or Newer** when attempting to register an EFT Serial number issued for v8.0.7 and later.

This option mainly affects the registration of EFT server since there are no differences between modules in Express or Enterprise.



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

attempts to register Cloud Connector Module, Perpetual and 8.0.6 or Older, the IcN display would be CCM.

**Additional notes:**

- The Advanced Registration Options are retained only for the current registration session. If you close the Registration Wizard or successfully register a module on any subsequent attempts, the previous configuration is not retained, and the EFT admin must reconfigure the Advanced registration details.
- If you want to undo the configuration, you need to close the Registration Wizard and relaunch the module registration to try again.
- Advanced Registration Options are not submitted on the registration request unless you make modifications to the Advanced Registration Options and click **OK**.
- Making changes and clicking **Cancel** will not submit the advanced registration options, and existing behavior is submitted to the registration server.
- When configured, and **OK** is clicked, the registration request will submit the configured IcN that is displayed in Advanced Registration Options along with the entered serial number.
- Only one request is made to the registration server instead of multiple requests; the IcN that is displayed in the Advanced Registration Options along with the entered serial number are submitted.

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

1. Complete registration information in the Registration Wizard, as usual:
  - Serial number
  - Registered to information on next page
2. Click the option to email registration request.
  - Ignore any message that says "could not find mail software." This action is to copy information into the clipboard.
3. Open up a text editor.

4. Paste the content from the Clipboard into the new blank text document.
  - The first line should say something about emailing; delete that line.
5. Save this document and transfer it to a computer that has Internet access.
6. Copy the information from the text document and paste it into the form found at this address: <http://www.sat.globalscape.com/register/>.
7. Click **Register Me**.
8. This will either download a REG file or output the information within the browser, depending on the browser that you use.
  - If it is in the browser, copy this and paste it into a new blank text document. Save it as a .REG file and move it back to the server computer.
9. With the service NOT running, double-click the REG file to merge the key to the registry.
10. Restart the EFT server service. When you log in to the administration interface, you should see that it is registered when you click **Help > About**.
11. Repeat these steps for any additional modules that need to be registered.

Alternatively, you can email the content of the Clipboard to [manreg@globalscape.com](mailto:manreg@globalscape.com). You will receive a .REG file from Globalscape Support.

## Windows Account for the EFT Server Service

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

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
- [map a virtual folder to a network drive](#)
- the Windows Registry

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 will be different; 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.
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. In **Administrative Tools**, click **Local Security Policy**. The **Local Security Policy** dialog box appears.
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**

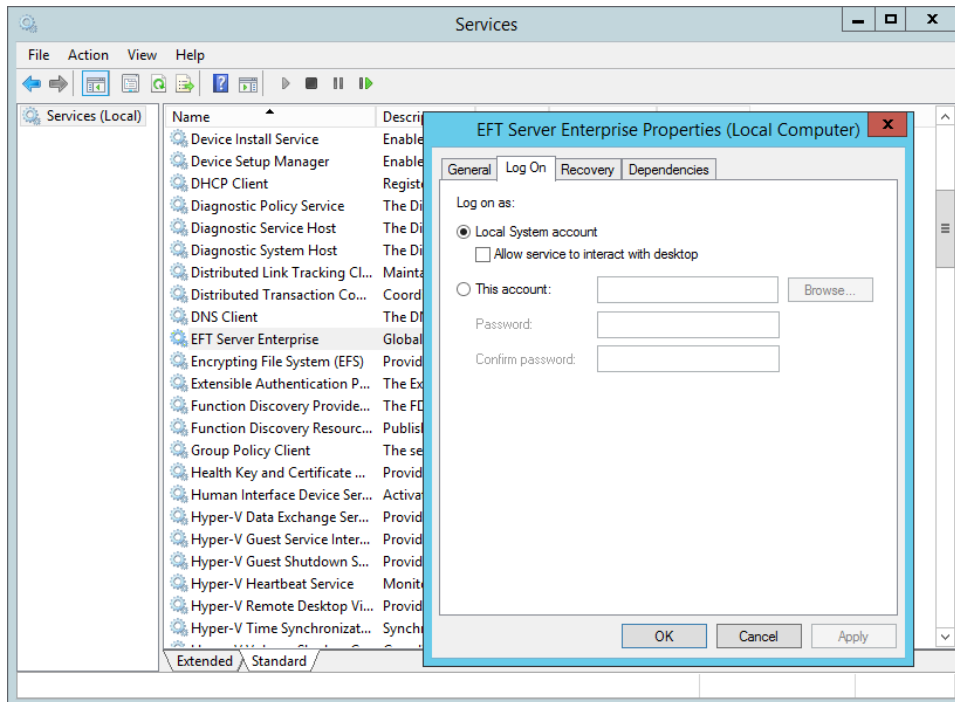
1. In Windows File Explorer, right-click the file or folder, then click **Properties**.
2. On the **Security** tab, click **Permissions**. The appearance of this dialog box is slightly different for files and directories and for different versions of Windows (W2K, XP, etc.).

For more information about setting permissions to folders and files, refer to the Windows Help documentation for your specific operating system. (for example, click **Start > Help and Support**, then search on keyword *permission*.)

# Assigning the Service to a Windows User Account

## To assign the service to a Windows user account

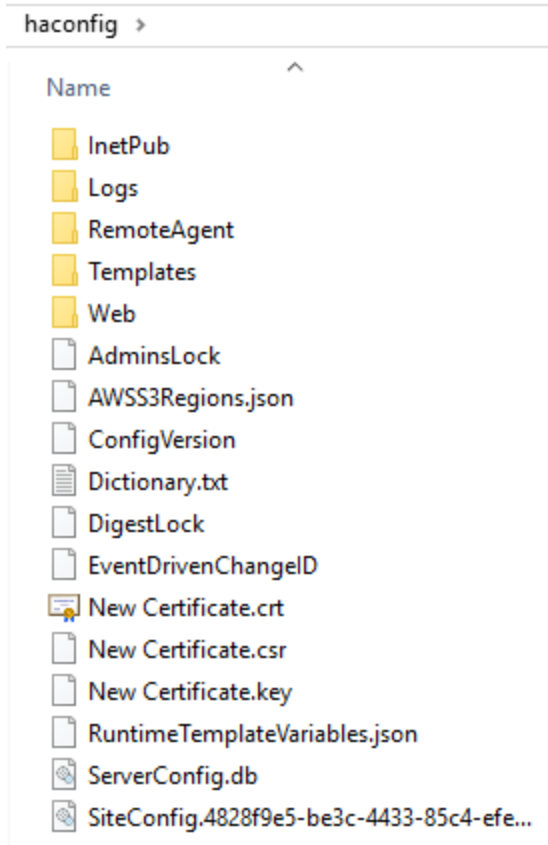
1. Click **Start > Run**, type `services.msc`, then press ENTER.
2. In the **Services** console, right-click the EFT server service, and then click **Properties**.
3. Click the **Log On** tab, then click **This account**.



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

# HA Nodes Configuration Files

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



- An Advanced Property was added to improve performance when configuration is copied to the cluster share. When off, `HAFullConfigDumpIntervalMins = 0` or is not defined, the full configuration is copied on each change. Add the Advanced Property and set it between 1-10 minute intervals to reduce network traffic.
- A local configuration path for each node must also be specified for each node for local caching. When configuration changes are made to SSH, trusted SSL certificates, OpenPGP key materials, and AML files ([Advanced Workflow](#) tasks), those files are cached locally, and uploads are safely synchronized to the [shared config path](#). The other nodes then update their local cache from the central location. Thus, the central share always contains the current version of those files. When, for example, a new SSL Cert or AML file is created, the creator directly adds/modifies the files on the network share then tells the other nodes that the file was modified/created and they need to update their local cache (that is, copy the file to their local ProgramData directory).

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

### Related Topics

- [Logging for HA Nodes](#)
- [HA FAQ](#)

# 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. Refer to [Can you remotely administer EFT without the administration interface?](#) for details.
- If you do NOT want to install the administration interface, but want to use the COM API remotely, refer to "Can you remotely administer EFT without the administration interface?" in [COM API online help](#).

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

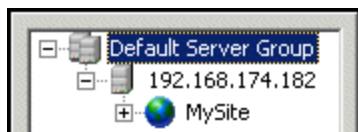
To install EFT and the administration interface on the same computer, refer to [Installing the Server, Interface, and Modules](#).

### **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.

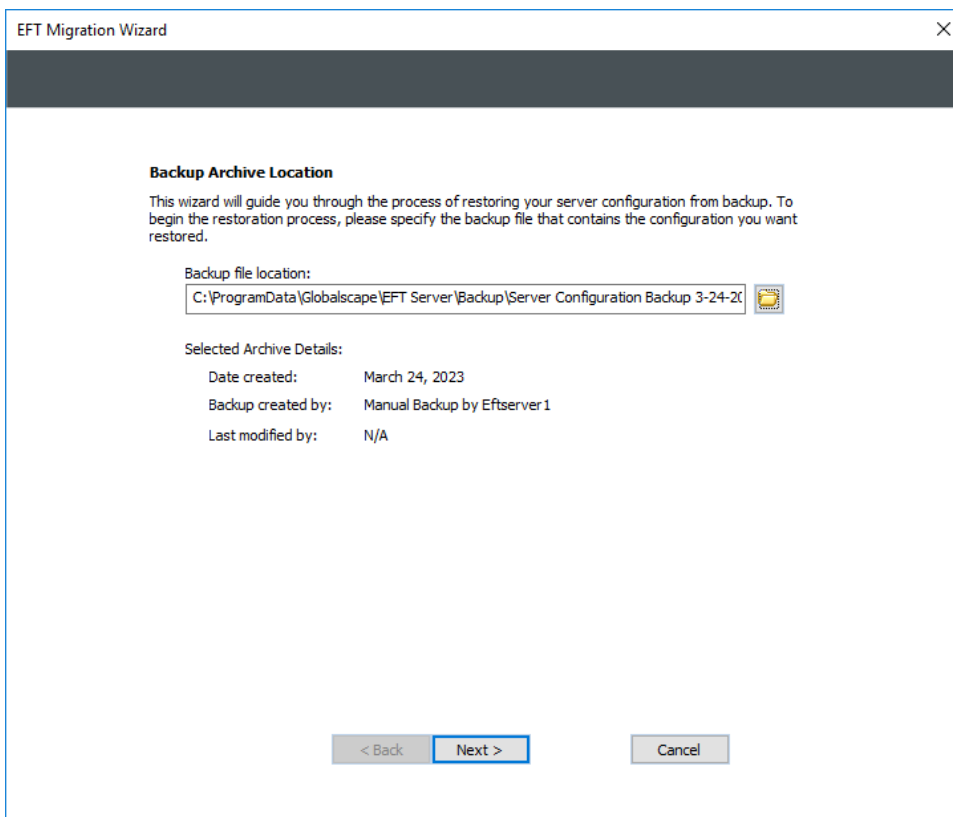
- If you want to review the version history in your default text editor, select the **Show version history** check box.
  - If you want to display the installation log, select the **Show installation log** check box.
11. Click **Finish**. The administration interface appears and the **EFT Server administrator 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.



# Backing Up or Restoring Server Configuration

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



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

- **Performing Disaster Recovery.** If the production Site is corrupted and configuration is lost, damaged, or destroyed, the wizard can assist you with restoring EFT to a prior working state.
- **Migrating from staging to production or to new hardware.** If you want to move EFT from a staging or development box to a production server or have set up a Server with one or more Sites on one computer and want to move it to another computer or a different network location, the wizard can assist you with gathering all the necessary files for a successful move.
  - If you are migrating from a test environment to a production environment and do not need to keep the test environment's Server, Site, and user configuration settings, you do not need to use the EFT Migration Wizard. You can just start from scratch, and run the Server, Site, and New User wizards on the new system.
  - The migration wizard will only accept **backups created with the same version** that is being restored to; using backups from different versions will not work.
  - To restore, you will use the login credentials of the server administrator that you are logged in as, regardless of the credentials used to back up the configuration.
- **Backing up for disaster mitigation (routine backups, or backup prior to major changes).** If you need a backup to be readily available and require automatic backup, the wizard can backup all of your settings. The EFT Migration Wizard can also help if a major change is about to be made, such as new hardware changes to the EFT computer, and you need a mechanism to manually backup the current configuration. The EFT Migration Wizard can take a snapshot immediately before the major change takes place, in addition to the automatic daily backups.

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

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

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

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

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

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

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

### To manually back up Server configuration

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

- If a "backup successful" message appears, click **OK** to dismiss the message.
- If a failure message appears, restart the EFT service, then run the backup again.

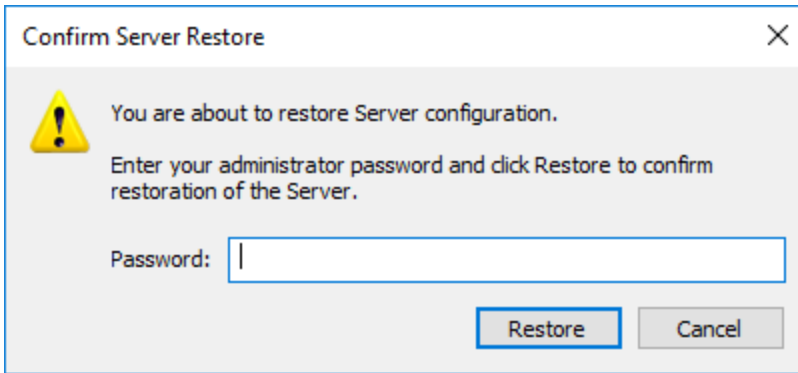
Any configuration changes made since the backup are, obviously, not included in the restore. For example, if you have deleted or added users since the last backup, those users will have to be deleted or added again after you restore.

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

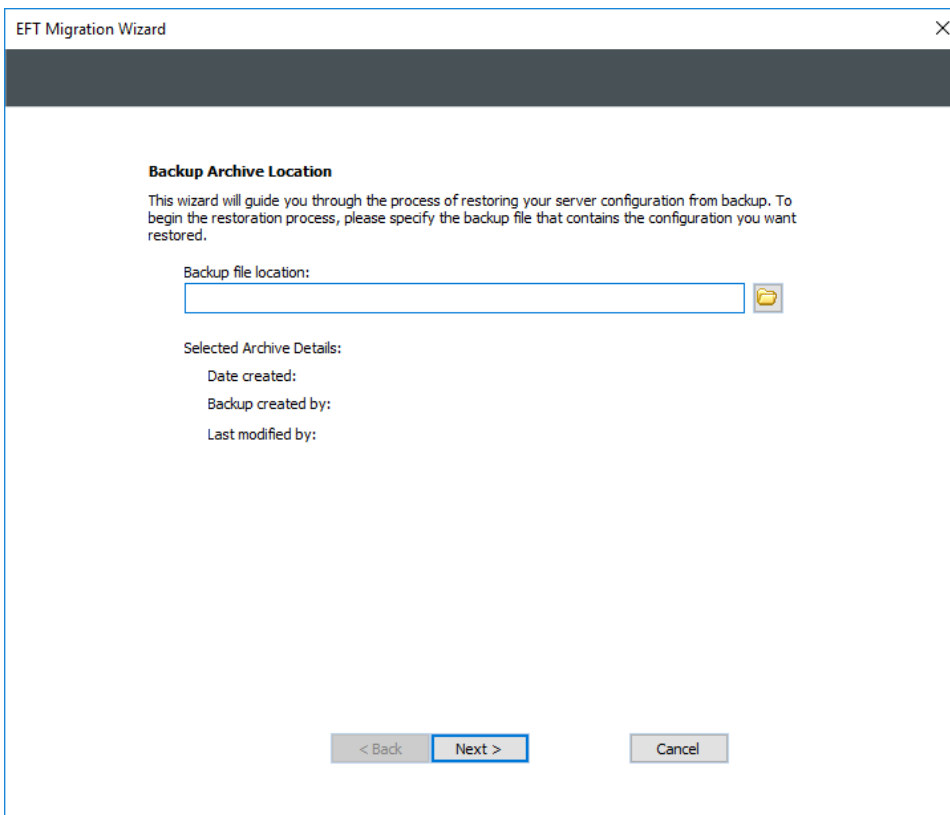
### To restore Server configuration

1. Install and activate the product on the target system, if restoring to a different computer.
2. After installation is complete, the **New Administrator Connection** wizard appears. You must configure the local connection (that is, create the LocalHost Server object in the tree) before you can restore from backup.
3. In the **Connection** wizard, leave **This computer** selected, and specify the **Label** for the local connection. By default, the label is `LocalHost`. Because LocalHost is a very common label, it is a good idea to change the label to something that is easily identifiable in error logs, reports, and remote connections. For example, `GS_EFTS`. You can label EFT anything you want; the EFT name is **not** dependent upon the computer name.
4. After you are logged in to EFT, do one of the following:
  - In the **Server Setup** wizard, click **Restore from Backup**.
  - On the main menu, click **File > Restore Server Configuration**.

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



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



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

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

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

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

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

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

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

If your EFT folder structure includes user folders (for example, C:\inetpub\EFTRoot\MySite\Usr\Recreate the entire folder structure check box and do not recreate these folders manually, the users will not be able to access their folders.

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

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

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

The **Server Administration Connectivity** page appears.

- b. Review the IP address for each Site. If you are restoring a Site to a different IP address, click to edit the IP address in the **New IP Address Assignment** list. The **Sites to Restore** page appears.
- c. Click **Next**. Select the check boxes of the Sites whose settings you want to import and clear the check boxes of the Sites whose settings you do not want to import.
- d. Click **Next**. In the **Site Listening IP Address Assignment** page appears. Click the links to specify one or more IP addresses to use (or All Incoming), and then click **OK**.
- e. Click **Next**. The **Site Authentication Manager Settings** page appears.

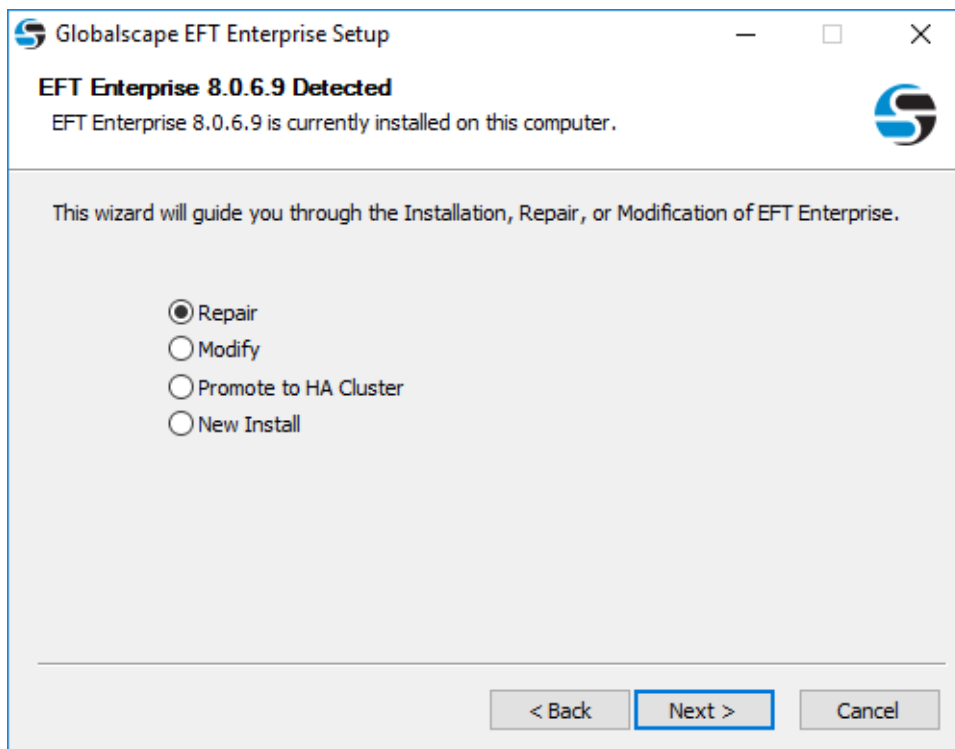
- f. The authentication database for each Site to be restored appears in the list. In the **Settings** column, click **View/Modify** if you want to view or change the path where EFT will store the user database. (You cannot change the type of authentication.)
- If EFT cannot connect to the Site's authentication provider, an error message appears.
  - Click **OK** to continue as is or click **Cancel** to modify the authentication provider settings.
- g. Click **Next**. The **Site Root Folder** page appears.
- h. Review the root folder location for each Site that you are restoring. If necessary, click the folder icon to specify a different location, and then click **Next**.
- i. If the DMZ Gateway is defined and configured in EFT that you are restoring, the **DMZ Gateway** page appears. If not, skip this step.
- i. Review the IP addresses and ports for the DMZ Gateway. Click to edit the IP address or port, if different.
  - ii. Click **Next**. EFT will test the DMZ Gateway connection and, if successful, the wizard proceeds to the next page.
    - If a failure occurs, the wizard displays a warning prompt indicating failure to connect to the DMZ Gateway and allowing you to either fix the problem (go back to the previous page to verify the IP address and port) or proceed anyway (if the IP address and port are correct, but the DMZ is not communicating).
- j. If the Auditing and Reporting module is defined and configured in EFT that you are restoring, the **Auditing Database Connectivity** page appears. If not, skip this step.
- Click **Test** to verify connectivity to Auditing and Reporting Module queue and, if successful, send a test message to the database. If a connection to the database cannot be made within 5 seconds, a warning prompt appears. (Verify that the database is available.)
- k. Click **Next**. Database connectivity is again verified and the **Ready to Restore** page appears.

- l. Read the information on the page, and then click **Restore**.
- m. A message appears indicating whether the configuration was successfully restored. Click **OK**.
- n. Review the log if errors were encountered during restore.

## Modifying or Repairing the Installation

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

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



### To modify or repair the software

1. Launch the installer. The installer will detect an existing installation.
2. Do one of the following:

- To upgrade the existing installation, click **Repair**. (**Repair** overwrites changed files and reinstalls missing files.)
  - To install or uninstall specific components, click **Modify**. (**Modify** installs selected components; removes unselected components.)
  - To install a fresh installation, including a new configuration file, click **New Install**.
3. Click **Next** and follow the instructions in the wizard. Refer to [Installing EFT, administrator, and Modules](#), if necessary.
  4. If you chose **Modify** in step 2, on the **Components** page, select the check boxes of components you want to install and clear the check boxes of components you want to remove. **If you clear the check box of an installed component, it will be uninstalled!**
  5. When the wizard is finished, restart the [Server services](#). The EFT service **Log On as** account will be set to **Local System** account by default. You can edit this in the service's **Properties** dialog box, on the **Log on** tab. (**Start > Run >**`services.msc`.)

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

## Promoting EFT Stand-Alone to Cluster Node

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

You cannot promote a stand-alone server to an existing cluster. In that case, you would have to reinstall EFT on the stand-alone box as a active-active server, using instructions in Globalscape Knowledgebase article #[11271](#), "Installing and Upgrading EFT in an Active-Active HA Cluster," and then point the new active-active server to the existing cluster configuration path.

# Upgrading EFT

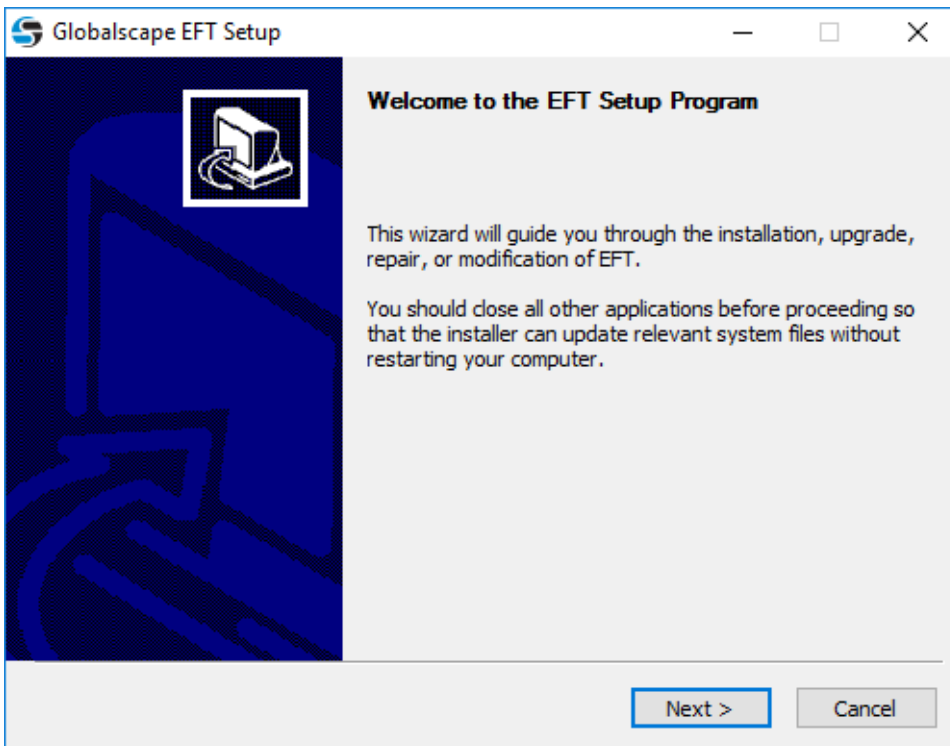
For a successful upgrade, it is important to understand the changes between your current version and the version you are upgrading to. In some cases, you will need to do a "stepped" upgrade, as you can't upgrade directly from some older versions to the current version.

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

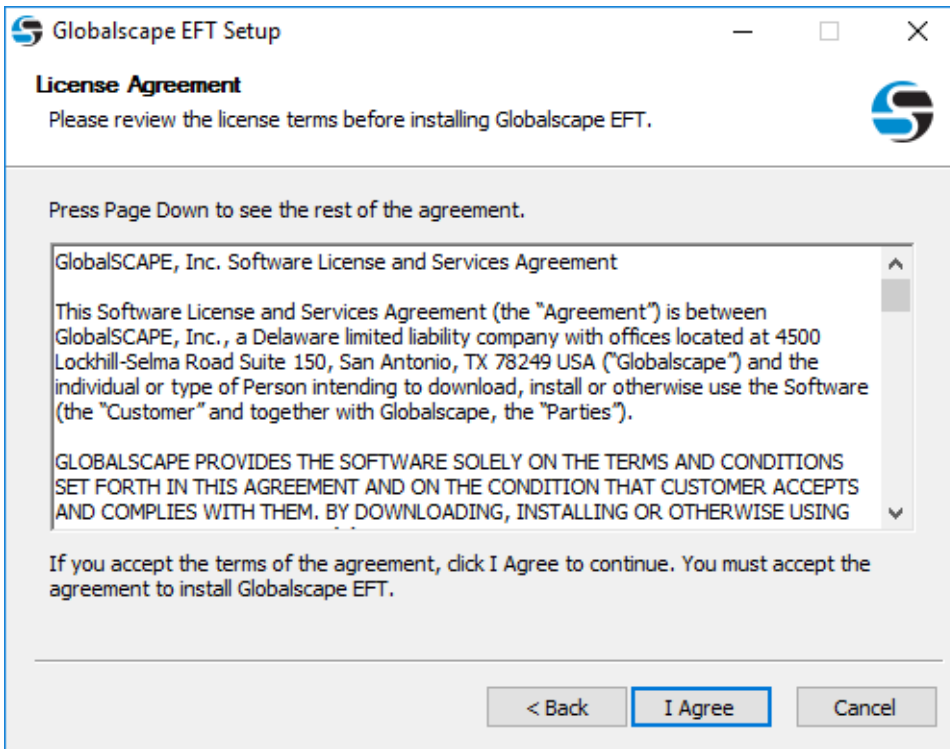
**Before upgrading your EFT installation to EFT v8.1, please read and understand the information provided in the Knowledgebase article [Upgrading to EFT v8.1](#).**

## To upgrade EFT and its modules

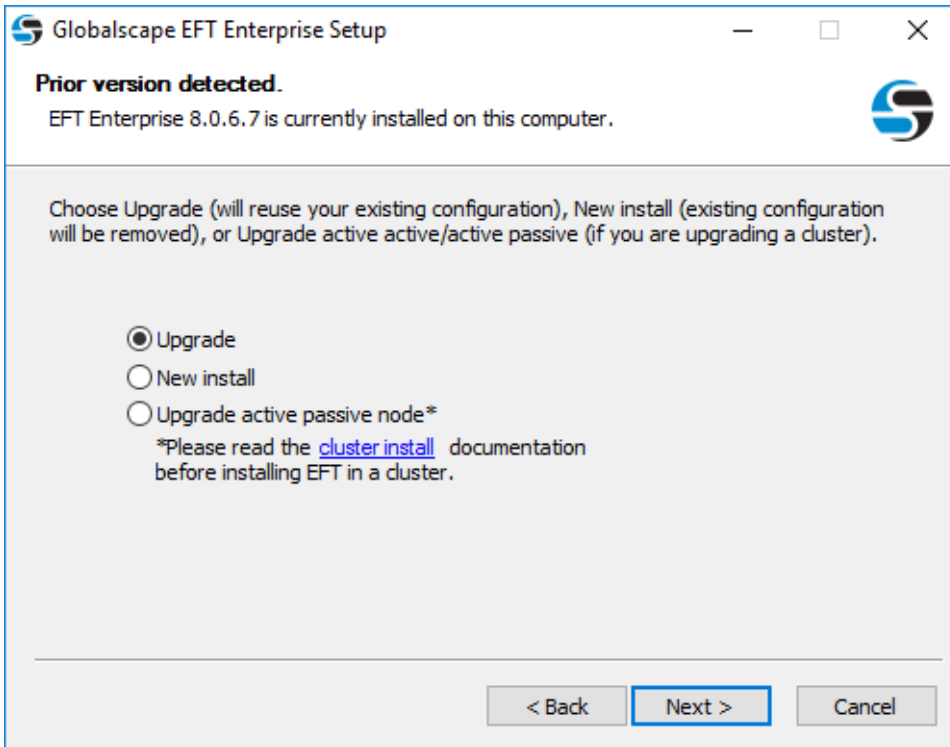
1. Close all unnecessary applications so that the installer can update system files without rebooting the computer.
2. Start the installer. The **Welcome** page appears.



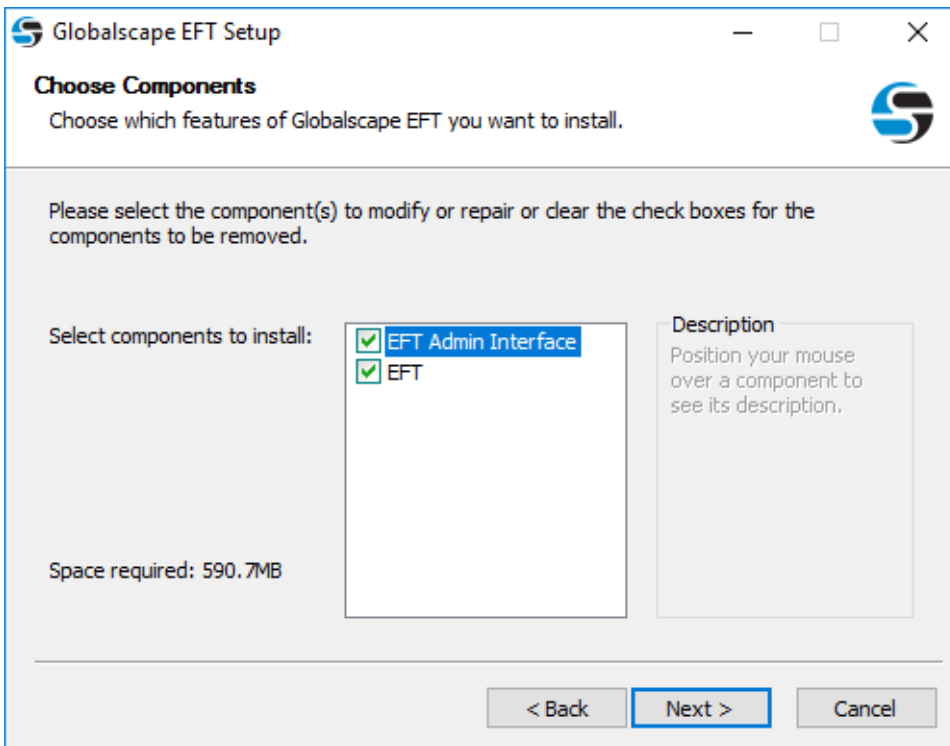
3. Read the **Welcome** page, and then click **Next**. The **License Agreement** page appears.



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

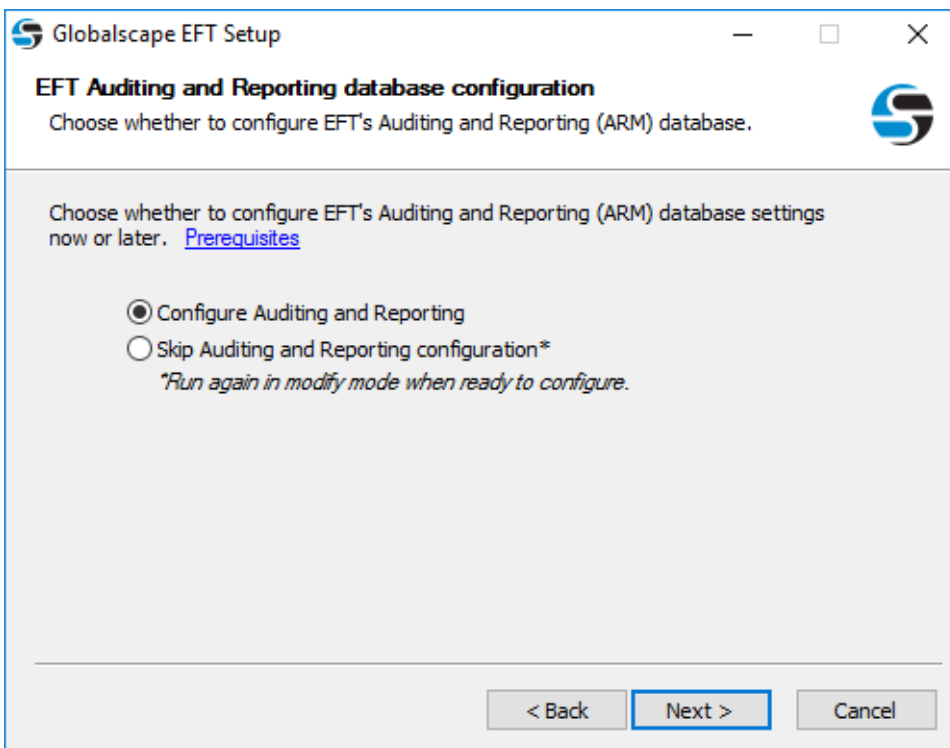


5. Click **Upgrade** then click **Next**. The **Choose Components** page appears.



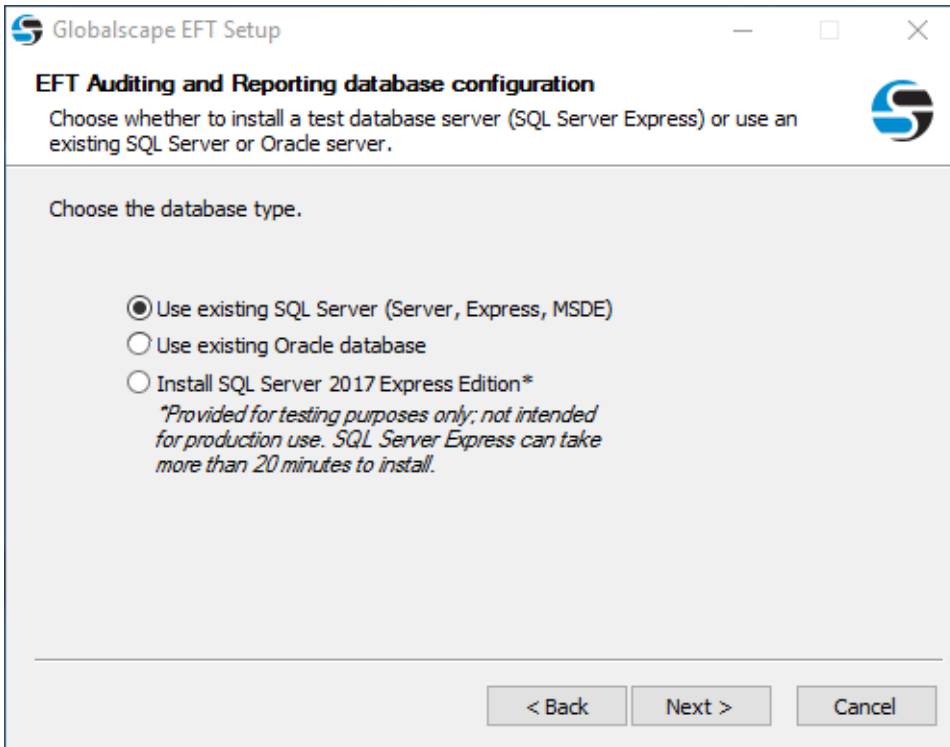
When you install EFT, the **EFT administrator Interface** check box must also be selected. After you have installed EFT and the administration interface on one computer, you can install the administration interface on other computers for remote administration. (To install the administration interface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

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



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

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



- **Install SQL Server Express**

- SQL Server Express is provided for use in a trial. It is not intended for production use. During installation, a default system administrator account (the "sa" account) will be created within SQL Server Express. The password is set to Password1.
- Click **OK** to continue SQL Server Express installation and follow prompts to complete SQL Server Express installation.
- Once the SQL Server Express installation begins, you can't cancel it. The only way to stop it is to reboot the computer.

- **Use existing SQL Server:**

**Globalscape EFT Enterprise Setup**

**EFT Enterprise Auditing and Reporting database configuration**

Choose whether to upgrade an existing EFT ARM database on the existing database server or to create a new one.

Specify whether to upgrade an existing EFT ARM database or to create a new one.

Create a new EFT ARM database  
 Upgrade an existing EFT ARM database\*  
*\*Please refer to the [ARM upgrade documentation](#) before upgrading*

< Back   Next >   Cancel

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

**Globalscape EFT Setup**

**EFT Auditing and Reporting database configuration**

Specify the database server's host address, the EFT ARM database name, the database owner credentials, and SQL Server authentication mode.

Please specify the database server's host address, the EFT ARM database name (EFTDB), the database owner credentials, and the SQL Server authentication mode.

Authentication Mode:  SQL  Windows

Database server host address or instance name:

EFT ARM database name:

Database owner username:

Database owner password:

< Back   Next >   Cancel

- b. Specify **Windows** or **SQL** Authentication. (**Windows** mode allows you to connect through a Microsoft Windows user account. **SQL** allows you to connect using either Windows Authentication or SQL Server Authentication.)
  - c. Specify the host address or instance name.
  - d. Specify the database server SA or privileged user account name (for example, sa).
  - e. Specify the database server SA or privileged user account password.
  - f. (Optional) Click **Next** or **Test** to test the connection to the database. If the test fails, click **Yes** to verify database connection details or **No** to continue without configuring the database.
- **Use existing Oracle database:**
    - a. Click **Create a new schema**. The configuration page appears.

The screenshot shows a window titled "Globalscape EFT Setup" with the subtitle "EFT Auditing and Reporting database configuration". The window contains the following text and fields:

Specify the Oracle database server's host address, database name, and database administrator credentials.

Please specify the database server's host address, database name, and database administrator credentials for creating the ARM schema.

Database host address (address:port)

EFT ARM database name:

User Name:

Password:

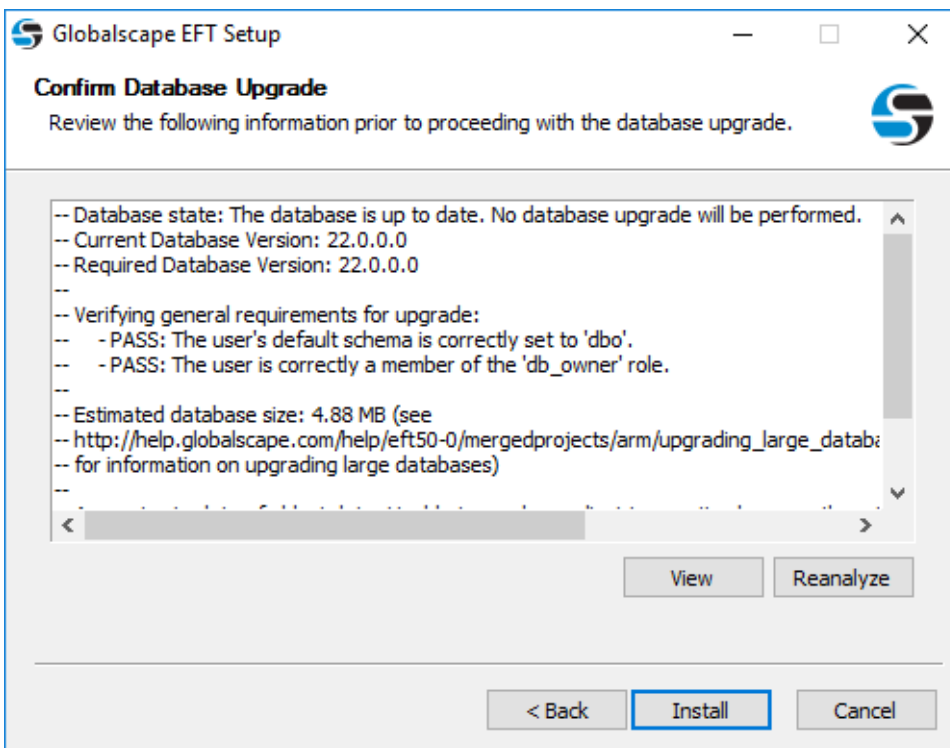
At the bottom of the window, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

- b. Specify the database host address and the EFT-specific schema name and database administrator credentials, and then click **Test** or **Next** to test the connection to the database. (If you have installed Oracle Database Express

Edition (XE) for testing/demo purposes, the instance name is XE and the User Name is SYSTEM.)

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

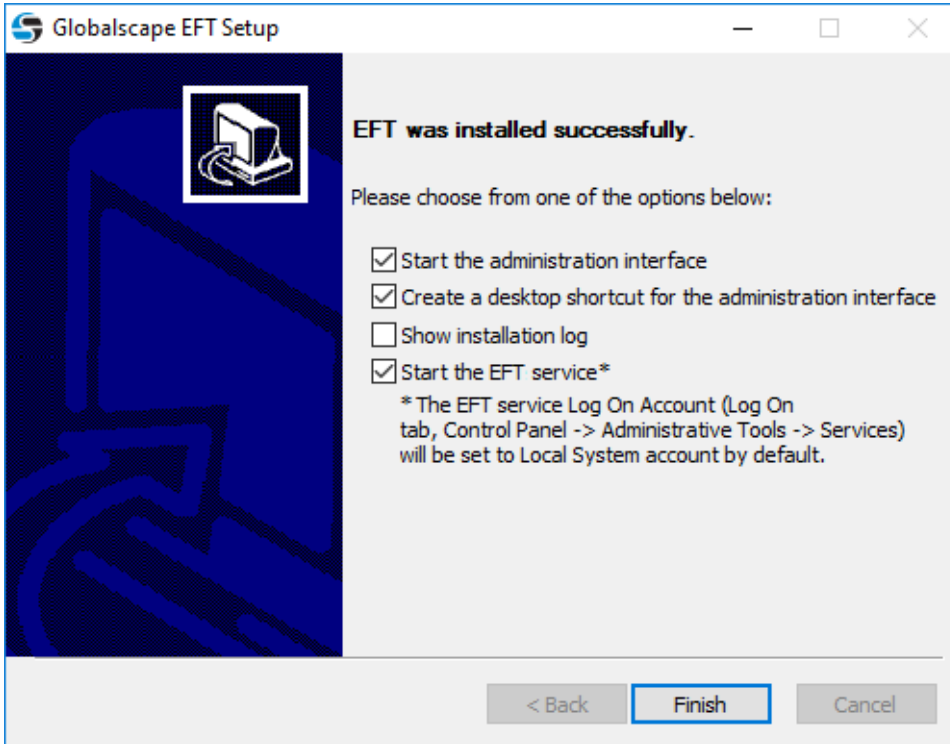
8. After the test is successful, click **Next**. The **Confirm Database Upgrade** page appears.



9. The database version information is displayed.

- Click **View** to open a TXT file of the database upgrade details and save the file for later, if needed.
- **Reanalyze** compares the new database information to the old and displays it on the page.
- Select the **I understand...** check box to continue, then click **Install**.
- Click **Install**. When installation is complete, a **Completed** page appears.

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

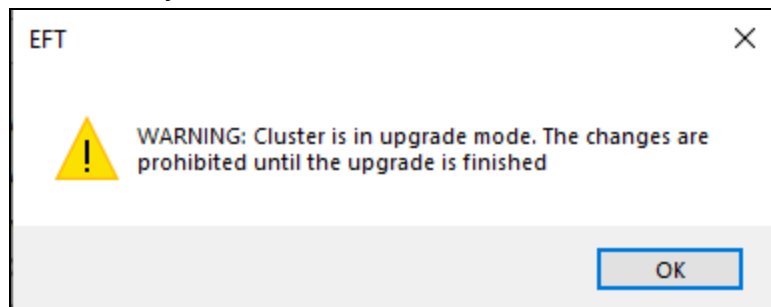


- Click **Finish**.

## Upgrade HA Nodes with Zero Downtime

In EFT v8.1 and later, EFT administrators can upgrade their HA nodes with "zero downtime," meaning you can upgrade a cluster without stopping all nodes at the same time.

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



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

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

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

- When enabling the upgrade, EFT administrators will be prompted with a warning that the transition and change cannot be undone.
- The warning prompt should reference details to review documentation.

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

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

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

Upgrade state limitations:

- Backup/Restore feature is prohibited
- No configuration changes are allowed during the Upgrade state, except moving the cluster back into the Normal state

- **Normal State.** Requires all nodes have the same version. Upon transition to Normal, the Upgrade State will display “Not Active”

Normal state limitations:

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

- Transition state from Upgrade to Normal are global, which affects all nodes within the cluster, so administrators should only end upgrades after all nodes have been upgraded.

The screenshot shows the 'High Availability' configuration window. The 'Upgrade State' is highlighted with a red box and reads 'Active; Outdated; version 8.0.8.0'. An 'End' button is visible next to the state text. Other configuration fields include 'Deployment Scenario' (MSMQ - Multicast), 'Multicast Address' (234.4.4.4), 'Multicast Port' (8444), 'Coherence Queue' (.private\$\EFTCoherenceQueue), 'Event Queue' (.private\$\EFTEventQueue), and 'Config Path' (\\pdc\Transfer\%\*\EFT).

The screenshot shows the 'High Availability' configuration window after an upgrade. The 'Upgrade State' is highlighted with a red box and reads 'Active; Updated; version 8.0.9.0'. An 'End' button is visible next to the state text. Other configuration fields are identical to the previous screenshot.

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

### Normal state to Upgrade state

- All nodes are Outdated. Admin logs in to any of the nodes and enter the cluster into the "Upgrade" state (with GUI/COM/REST).
  - EFT admins shall be able to transition from Normal to the Upgrade state via our EFT administrator interface High Availability tab.
  - EFT admins shall be able to transition from Normal to the Upgrade state via COM. Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade.
  - EFT admins shall be able to transition from Normal to the Upgrade state via REST API. Appropriate error message(s) will be provided if enabling Upgrade state on any node when the cluster is already configured for Upgrade.
  - The ability to start the Upgrade state is a global setting; once set at any node, all nodes will report the same state.
  - Upgrade state should be used ONLY when upgrading to a new version of EFT and not when an EFT administrator forgets to upgrade a node in the cluster from a previous upgrade.
- Once configured for Upgrade, the cluster is in Upgrade state, and you can upgrade each node one by one.
- Outdated nodes write audit data to local \*.sql files only; Each node will have their own local \*.sql file.
- Updated nodes write into ARM database; If no SQL schema changes exist, there is a post process in the Normal state that will migrate the data from the \*.sql file into the ARM database.
- Uses Web folder appropriate to node's version.

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

### Upgrade state to Normal state

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

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

### **COM has several methods to manage cluster upgrade state**

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

# Uninstalling the Software

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

## To remove EFT

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

## For a "Clean" Uninstall

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

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

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