globalscape
by HelpSystems

EFT v8.0.7 Installation and Implementation Guide

Copyright Terms and Conditions

Table of Contents

Installing EFT and Modules

The instructions below describe how to install EFT.

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

Before You Begin

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

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

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

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

Before installation

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

System Requirements

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

(See also 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 2019
    - Windows Server 2016
- Free RAM:
    - **Minimum**: 4 GB free RAM
    - **Recommended**: 8 GB free RAM (moderate AWE usage)
    - **High Performance**: 16GB free RAM (if AWE is extensively used)
    - 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 or later (all components, including AWE, AS2, and SQL Server require .NET Framework)
- 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)
    - 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 Samba network shares, version 3.x or later of Samba
- 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, AWE, and AS2 requirements below if you plan to use those modules remotely.)

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

  The installer includes SQL Server Express (intended for evaluation purposes only). EFT is supported with the following SQL Server versions:

  - SQL Server 2016
  - SQL Server 2017
  - SQL Server 2019
- Microsoft® ActiveX Data Objects (ADO)
  - EFT uses Microsoft ActiveX Data Objects (ADO) 2.7 or later to handle database communication, which in turn should load the Oracle drivers to handle Oracle implementation details. How and what is connected largely depends upon the connection string. By default (if you do not supply the entire connection string in EFT), the Oracle connection string should look like:

```
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};
```

- Oracle requires EFT; refer to Oracle's documentation regarding Oracle system requirements. Be sure to reboot after you install the Oracle Data Access Components (ODAC). You need to use the 32-bit ODAC, even if EFT is installed on a 64-bit operating system. EFT supports the following Oracle versions:
  - Oracle Database 12c Release 2 (12.2.0.1)
  - Oracle Database 18c (18.1.0)
  - 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
- Insight requires a SQL Server database; it does not work with Oracle databases

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

DMZ Gateway Requirements

- Refer to System Requirements for DMZ Gateway.
- EFT and DMZ Gateway cannot be installed on the same computer/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 Engine Requirements

- AWE v10 requires Microsoft .NET Framework 4.0 and EFT v7.4.5 or later.

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 5.0.0-20208241408
  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 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
Protocols	FTP/S (SSL/TLS), SFTP (SSH2), HTTP/S, and AS2 (Certain protocols other than FTP require optional modules.) • FTP Commands Supported by EFT • The FTPS protocol in EFT is compliant with RFC4217, "Securing FTP with TLS." • EFT supports SFTP versions 2, 3, 4, and 6. The outbound client defaults to version 4, and it is not configurable through the GUI, but can be configured in advanced properties. The EFT outbound client negotiates the SFTP version with the receiving server during session establishment. That is, if the receiving server only supports version 2, EFT Server will negotiate down and operate at version 2. • SFTP hashing algorithms supported: For both FIPS and non-FIPS ciphers and algorithms, refer to SFTP FIPS.
SSH version	EFT v8.0 and later use v8.1.0.0_openssh library, including OpenSSH DLLs for FIPS EFT's SFTP library implementation is based on the latest (8.1) version of OpenSSH portable: https://github.com/PowerShell/openssh-portable, which is a fork of https://github.com/openssh/openssh-portable, which in turn is a fork of the canonical OpenSSH. EFT will be updated once the fork that EFT is using is updated to 8.2, 8.3, or newer version. Also note that the EFT implementation contains some modified OpenSSH files, modified via use of a Fedora patch, for purposes of FIPS certification when FIPS mode is enabled.
SSL version	EFT v8.0.6 and later use OpenSSL v1.1.1k; EFT v8.0.4 and later use OpenSSL v1.0.2u (dated December 20, 2019), SSL.dll and SSLfips.dll; EFT v8.0.0 - v8.0.3 use OpenSSL v1.0.2t; TLSv1.2 is set by default. For best security, clear versions that you do not need enabled; do not enable SSLv3 ciphersuites (See FIPS description below.)

Item	Description
FIPS	EFT uses the FIPS Object Module; https://csrc.nist.gov/publications/detail/fips/140/2/final; https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2839; (In addition to the validations of the OpenSSL FIPS Object Module 2.0 obtained directly by OpenSSL, third-party vendors have obtained additional "re-brand" validations of the same cryptographic module. #2939 is referenced to show all of the algorithms covered.) • OpenSSL v1.0.2 is FIPS-certified, but does not support TLS 1.3. EFT uses v1.0.2 for SFTP in FIPS and non-FIPS mode because SFTP doesn't care about TLS version OpenSSL v1.1.1 has no FIPS module, but supports TLS 1.3; EFT uses it in non-FIPS mode to support TLS 1.3
SSL Certificate Key lengths supported	Key lengths supported: 1024, 2048, 3072, and 4096 bits
EFT-created SSL certificates	x.509 base-64 standard DER encoded
Allowed OpenSSL ciphers for inbound transfers (HTTPS and FTPS)	Refer to the **Server > Security** tab for available ciphers.
Authentication types	Built-in, AD/NTLM, LDAP, ODBC, RADIUS, RSA SecurID®
Log formats	W3C, Microsoft IIS, and NCSA
OpenPGP version	EFTv8.0.5 uses IP*Works! OpenPGP2020 v20.0 build 7525 components for secure OpenPGP messaging and advanced encryption/decryption (http://cdn.nsoftware.com/help/IGB/cpp/) and is RFC 4880 compliant.
PCI DSS	EFT facilitates compliance with PCI DSS version 3.x.
AS2 module	EFT uses /n software's EDI Integrator library components, which are in the core of an application called RSSBus. RSSBus is Drummond Certified and in compliance with RFC4130. (EFT itself is not Drummond certified.) The maximum inbound file size for AS2 transfers is 20GB; there is no limit on outbound file size.
Advanced Workflow Engine (AWE) version	EFT v8 uses Automate Desktop v10.7.100 Build 4 Task Builder and actions
ICAP/Content Integrity Control	EFT supports RFC3507, sections 3.2 and 4.9. EFT supports: draft-stecher-icap-subid-00 section 4.5 and 4.6.
EFT Outlook Add-In library	EFT v8.0.6 and later use Apache log4net v2.0.12

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.

Upgrading Notes

Refer to Upgrading to Continuum in the Knowledgebase before upgrading to v8.0.7. For information about upgrading EFT to versions before v8.0.7, refer to the Globalscape Knowledgebase topic #11194 .

Upgrading notes for v8.0.7:

- Each of the features you currently have registered will still be licensed/registered after upgrading (just packaged differently or renamed per the Features Availability table).
- If you want to register a new module, please register EFT "core" first to avoid any problems

Upgrading notes for v8.0.6:

- In EFT v8.0.6, the installer includes SQL Server Express 2019; Upgrades will continue to use SQL 2017 Express as we do not upgrade SQL Express via our installer
- When upgrading to v8.0.6, EFT will convert the reply behavior for File Uploaded rules from synchronous to asynchronous by default. This may affect the flow of existing File Uploaded rules. If needed, you can return to the legacy synchronous reply behavior by setting the Advanced Property 'WaitOnFileUploadEventCompletionBeforeSendingResult" to true.
- Upgrade can fail when multiple actions (>100+) exist in a single event rule. Setting up event rules like this can exceed transfer storage size limit and prevent importing event rules with a "big body." Workaround is to separate the event rules to have fewer actions or to increase EFT computer power. (Globalscape Professional Services can assist you in optimizing your event rules for better performance with their EFT Automation Assessment.)
- The EFT installer does not detect the App Data directory if the previous version was installed from a command-line (Silent Installation). You must upgrade using the same method.

Upgrading notes for v8.0.5:

- Upgrade 8.0.0.38 to 8.0.5.12 fails due to database upgrade functions. The workaround is a version-stepped upgrade.

  Copy the **\web** folder from the EFT installation folder to the cluster share (%ClusterShare%)

- Upon upgrade, the file structure of the EFT client location, **C:\Program Files (x86)\Globalscape\EFT Server\web\public\EFTClient\shadowfax\wtc\assets**, has changed to **C:\Program Files (x86)\Globalscape\EFT Server\Web\Shadowfax\wtc\assets** (**\public\EFTClient\** no longer exists) and the **admin-configuration.json** file has new parameters.
- Upon upgrade, the TLS Settings dialog box may be blank due to the changes in SSL between versions.
- If used in a previous version, the advanced property UserAgentHeaderSkipOTP will need to be updated in the JSON file to add brackets around the value, even if only one value is specified: "UserAgentHeaderSkipOTP": ["value"] Until the brackets are added, the advanced property will fail to load.
- In the WTC, the Progress icon continues to spin, even while an upload is paused
- In the WTC, the Password Reset functionality is not available for AD or LDAP
- After an upgrade of HA primary node, the modified theme.json file is not moved to the shared folder
- Twilio verification test option requires +1 before it can successfully send a test
- For the Acceleration module, pre EFT v8.0.4 scClient is NOT backward compatible with the DMZ Acceleration library with a trial expiry date of 11Jan21 (DMZ 3.5.0.24) and later. So, if a customer who's already using an older (pre 3.5.0.24) DMZ wishes to trial Acceleration using scClient, they will need to update the FAST dll in DMZ AND update their scClient on the EFT server.
- Upgrading to this version will convert all event rule actions set to run in synchronous mode, to asynchronous mode. This potentially can impact the logic/flow of client event rules after upgrade. In particular, the On User Login event rule can prevent users from logging in after upgrade, if it contains actions that get converted to sync mode and the action takes some time to complete. The current list of actions that support asynchronous mode are listed below. These actions will convert to synchronous mode.
    - Execute command
    - Execute Advanced Workflow
    - Send notification email
    - Call event rule subroutine
- When you upgrade from an earlier version, your event rules will have been changed to the new naming of the actions. For example, the Copy/Move Action from earlier versions is now the Protocol: Upload action.

Upgrading from EFT v7.4.x to EFT v8.x

The following changes upon upgrading from v7.4.x to v8.x should be noted:

- **EFT Insight**
    - EFT v8.0.x works with EFT Insight v1.0.7.4550 or later
- **Advanced Workflow Engine**
    - The Advanced Workflow tasks in versions prior to v8 were stored on EFT in the form of AML files. In v8 and later, they are stored in the SQLite database files. If you are using the **Task** Action in AWE, which is an AWE task that is calling another AWE task, you will need to export the AML files to a location that EFT can access.
- **WTC/Workspaces**

    - Customizations in the v7.4.x client interface do not carry over upon upgrade to v8.x. You should back up everything BEFORE upgrading, then you can apply your custom logo, theme.json file, and any customizations after the upgrade.
    - Some portals were not updated with the new look and feel. Those changes are expected in subsequent releases.
    - In v8.0.0 and 8.0.1, the send portal does not provide an option to select files in your Workspace; you can only select files on the hard drive. In v8.0.2, you can select Workspace files.
    - EFT v8.x does not support UPLOADS from CAC-authenticated users when using Chrome or Edge browsers. Firefox (and possibly other browsers) will work.
- Administration Interface
    - The **Site > General** tab and **Server > General** tab (anywhere that **Last modified by** is displayed) will report **Last modified by** as "EFTUpgrade" after upgrading
    - The **Site > Workspaces** tabs have been consolidated into the **Site > Web** tab
    - On the **Server > General** tab, the **Server configuration settings** box is not editable. EFT configuration is now stored in a database file.
    - Removed email address from **User > General tab**
    - Optional permission on **Server > administration** tab to give administrator accounts permission to manage personal data for users
    - Added User Account Details Template on **Site > Security** tab to apply GDPR-related privacy settings to all user accounts on a Site
    - Added ability to resize SSH Key Manager dialog box and Advanced Workflow dialog box
- SSH keys
    - Upon upgrade from 7.4.x to 8.x, ALL SSH keys are moved into each Site-specific key manager
    - The SFTP private key is pulled from the key manager
    - Upon upgrading to v8.0.4, EFT will enable the following ciphers:
        - aes256-gcm@openssh.com
        - aes128-gcm@openssh.com
        - rijndael-cbc@lysator.liu.se
        - aes192-ctr
        - aes192-cbc
- OpenPGP
    - OpenPGP key pairs are defined and managed on a Site instead of the Server
    - PGP keyring (pubring.pgp and secring.pgp) are stored in SiteConfig<GUID>.db
    - At EFT server service startup, a PGP folder is created in the **\ProgramData\Globalscape\EFT** folder
    - Upon upgrading from a 7.4.x version to EFT v8, ALL PGP keyrings are cloned into each Site keyring
    - Upon upgrading a legacy server, keyrings are cloned into each site keyring.

    - Added "Sites" combo box to OpenPGP Keyring dialog box; Removed "Sites" combo box from **OpenPGP Key Generation** wizard; Removed **OpenPGP Settings** dialog box.
- **VFS**
    - The VFS tree items (permissions and Virtual Folders) are saved in SiteConfig<GUID>.db
    - Encrypted folders settings should persist in SiteConfig<GUID>.db
    - Upon EFT server startup, previous versions of FTP.cfg are automatically moved to SiteConfig<GUID>.db and ServerConfig.db
- **Advanced Properties**
    - Non-default registry settings are moved to AdvancedProperties.json
    - EFT caches all Advanced Properties on service startup and purges legacy Advanced Properties from the registry
    - The following registry keys have been removed from the Advanced Property list
        - AppDataPath
        - DefaultCfgPath
        - Cluster and SharedFolder; these two are located in Cluster.json now
- **HA Configuration**
    - In EFT v8.x and later, you have the option to store logs on the cluster shared drive; the log naming convention now allows for that
- **EFT Configuration - Upon upgrade, EFT settings are transitioned from SiteConfig<GUID>.db and ServerConfig.db**
    - These Server-level settings are now stored in SiteConfig<GUID>.db
        - General Tab
        - administration Tab
        - Security Tab
        - SMTP Tab
        - Logs Tab
        - HA Tab
        - CIC Tab
    - These Site-level settings are now stored in SiteConfig<GUID>.db
        - General Tab
        - Connections Tab
        - Security Tab
        - Gateway Tab
    - EFT will request administrator credentials on Server Config Restore. If credentials are invalid, restoration will fail.
    - Restore from previous versions of EFT are forbidden. EFT now only supports restoration from the same version of EFT.
- **ODBC**

    - When upgrading from 7.4.x to 8.0.x, the ODBC schema has changed. If you are using ODBC as the authentication database, then you will need to consult with Globalscape Support so we can assist with the manual process necessary to get EFT updated and running.
- LDAP
    - LDAP search timeout now applies also to search timeout. The default value is 60 seconds.
- SFTP
    - When you create a Site, you are able to specify the use of SFTP and browse for a key. After the Site is created and you click on **SFTP config** (on the **Site > Connections** tab), you cannot browse the file system to find a key. Instead, you are taken to the SSH Key Manager.
- Content Integrity Control (CIC) Action
    - Upon upgrade, legacy server level CIC profiles will be cloned into each Site. CIC profiles are now site-level
- Remote Agents
    - When upgrading a GA EFT Server 7.4.13.15 to the latest 8.0 EFT Server, Remote Agents will not auto-update to the new version. You need to have the patched Remote Agent msi and executable before you can update to the latest 8.0 agents. You will need to enroll the agents with the patched versions before proceeding.

Installing and Activating 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.

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.

Active-Active HA Cluster—Installing or Upgrading the Server

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

Promoting EFT Stand-Alone to Cluster Node

In EFT v8.0.5 and later, 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.

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:

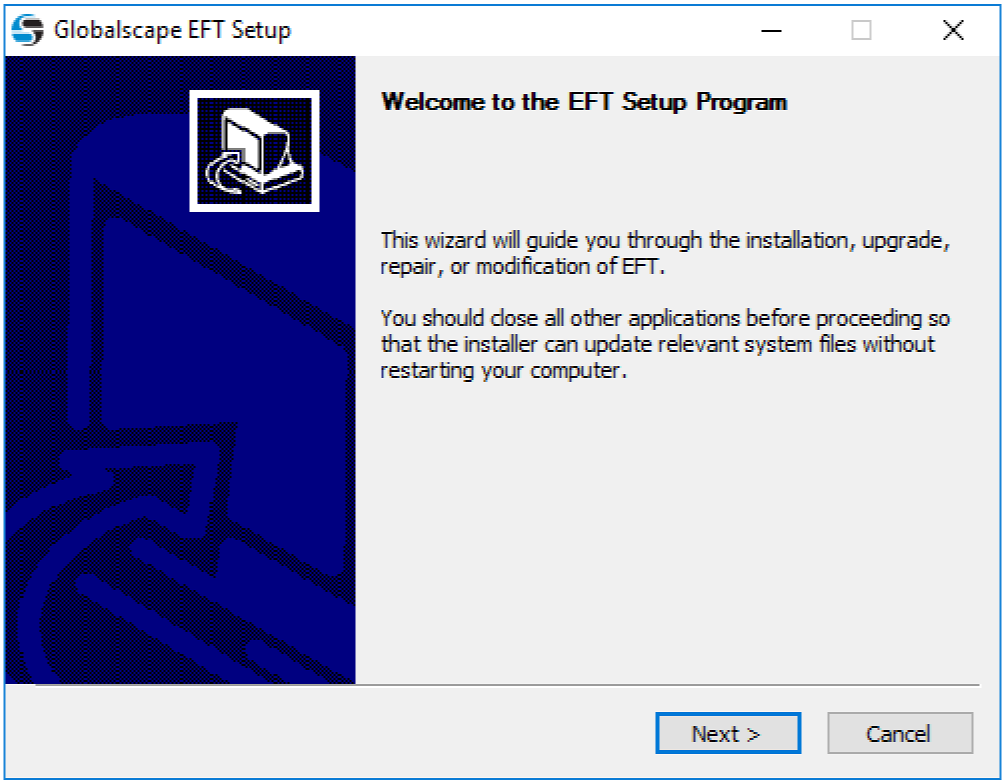
- **Before installing the software**, refer to System Requirements, and read the entire installation procedure below.
- After you have installed the system on a test computer and are now ready to move it to a production environment, refer to Backing Up or Restoring Server Configuration if you want to keep the test environment's Server, Site, and user configuration settings. Otherwise, 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. For details of installing SQL Server, refer to the SQL Server Install pages on technet.microsoft.com.
- The installer does not support Unicode characters. Refer to Unicode Exceptions for details.
- The EFT installer includes the ARM database installation/upgrade. If you want to install/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.
- **Before upgrading EFT**, to be able to see the AWE information in Insight, you must upgrade Insight to v1.0.5 or later so that the AWE tables are created in Insight.

The installer verifies that the following items before continuing:

- OS compatibility
- Is the user an administrator?
- DMZ Gateway is ***not*** installed on this server?
- .NET 4.0 Full 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.

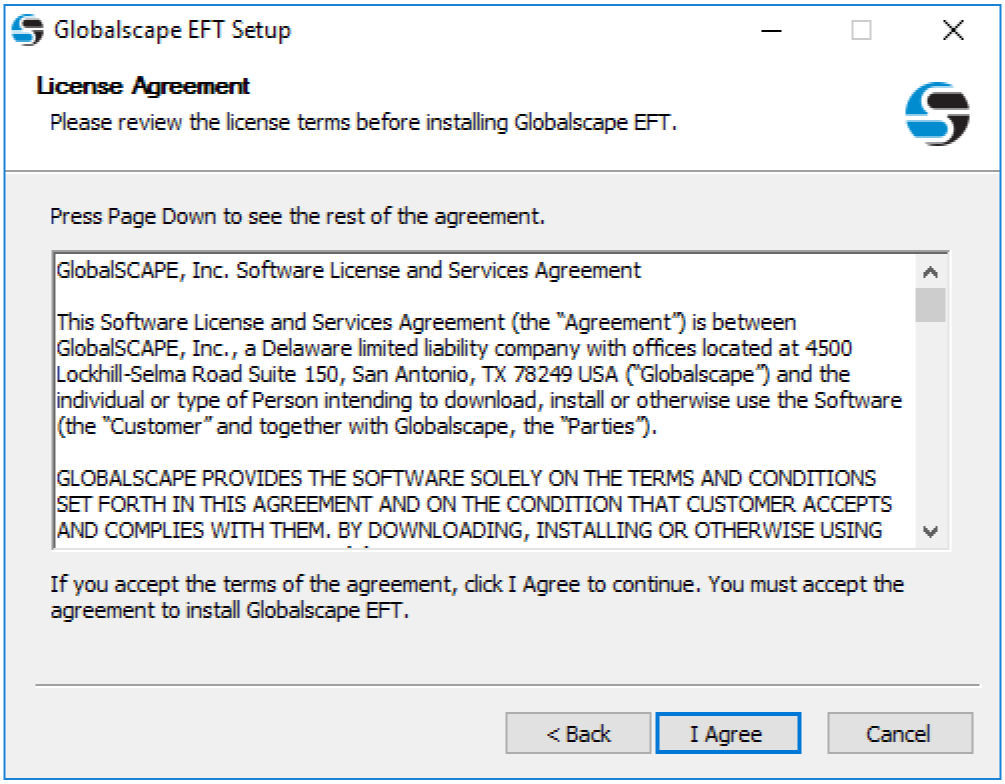


Welcome to the EFT Setup Program

This wizard will guide you through the installation, upgrade, repair, or modification of EFT.

You should close all other applications before proceeding so that the installer can update relevant system files without restarting your computer.

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



License Agreement

Please review the license terms before installing Globalscape EFT.

Press Page Down to see the rest of the agreement.

GlobalSCAPE, Inc. Software License and Services Agreement

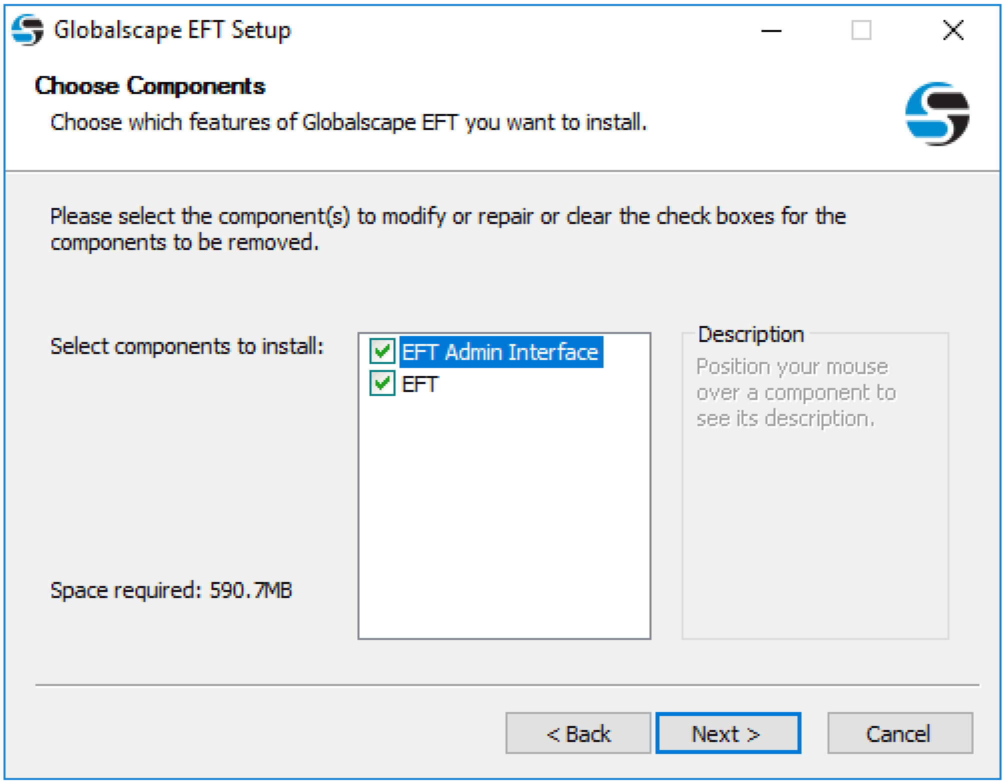
This Software License and Services Agreement (the "Agreement") is between GlobalSCAPE, Inc., a Delaware limited liability company with offices located at 4500 Lockhill-Selma Road Suite 150, San Antonio, TX 78249 USA ("Globalscape") and the individual or type of Person intending to download, install or otherwise use the Software (the "Customer" and together with Globalscape, the "Parties").

GLOBALSCAPE PROVIDES THE SOFTWARE SOLELY ON THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT AND ON THE CONDITION THAT CUSTOMER ACCEPTS AND COMPLIES WITH THEM. BY DOWNLOADING, INSTALLING OR OTHERWISE USING

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Globalscape EFT.

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.



Globalscape EFT Setup

Choose Components

Choose which features of Globalscape EFT you want to install.

Please select the component(s) to modify or repair or clear the check boxes for the components to be removed.

Select components to install:

☑ EFT Admin Interface
☑ EFT

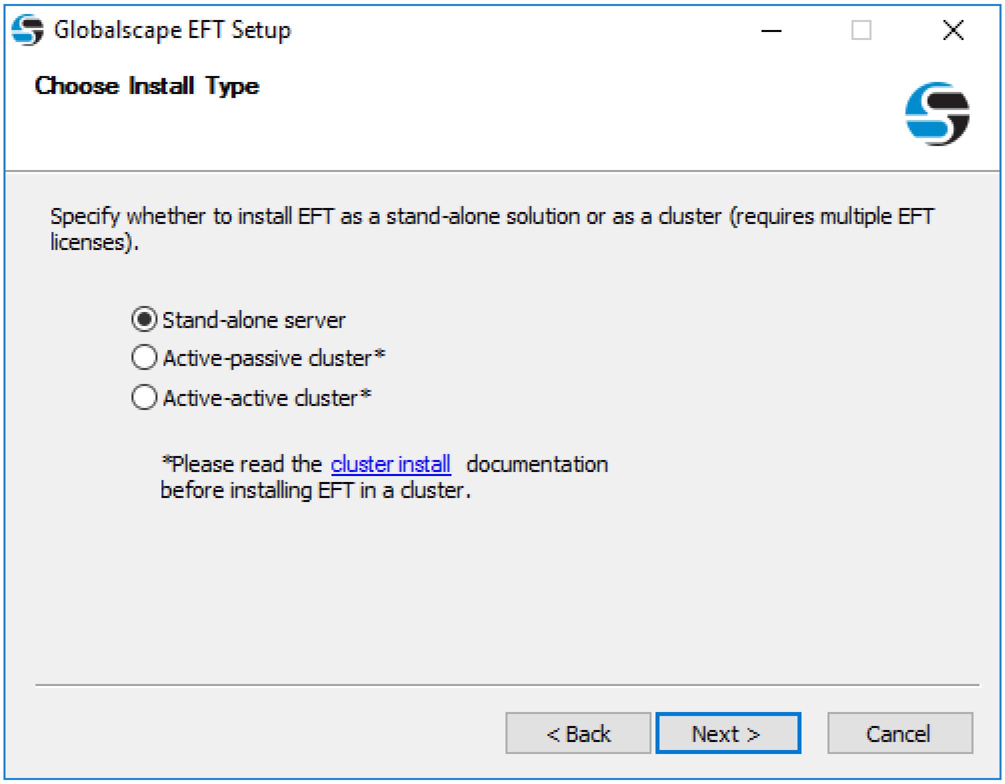
Space required: 590.7MB

Description

Position your mouse over a component to see its description.

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.)

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



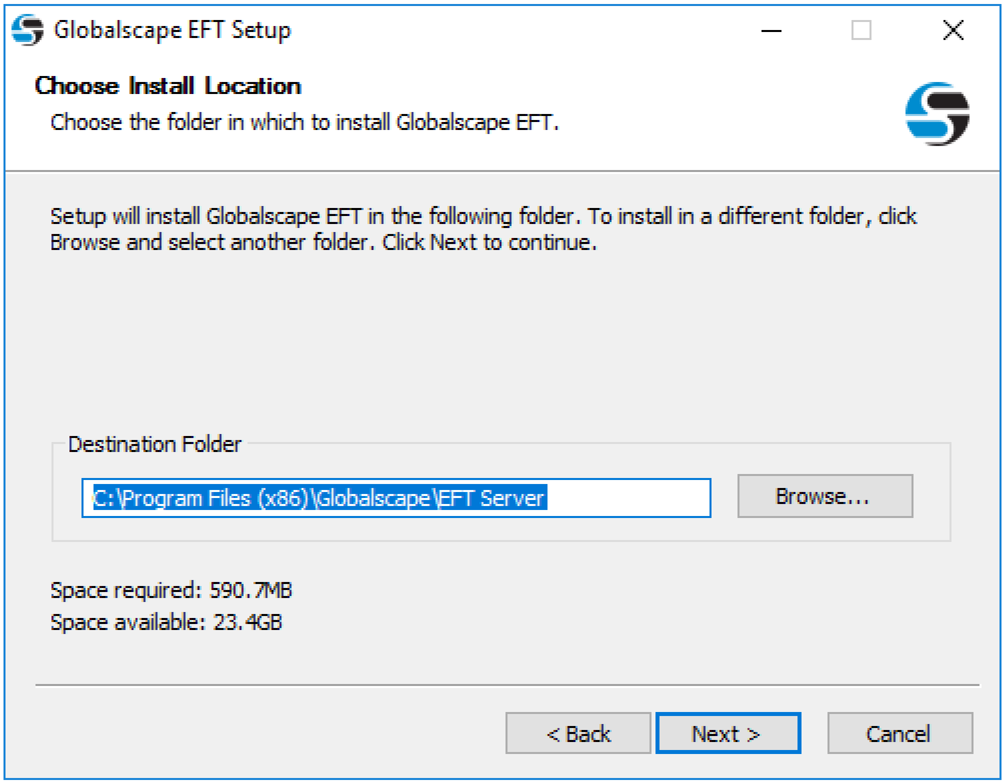
Specify whether to install EFT as a stand-alone solution or as a cluster (requires multiple EFT licenses).

● Stand-alone server
○ Active-passive cluster*
○ Active-active cluster*

*Please read the cluster install documentation before installing EFT in a cluster.

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. Refer to Installing or Upgrading the Server in a Cluster for the procedure for installing EFT in a cluster setup.
   - 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.



Globalscape EFT Setup

Choose Install Location

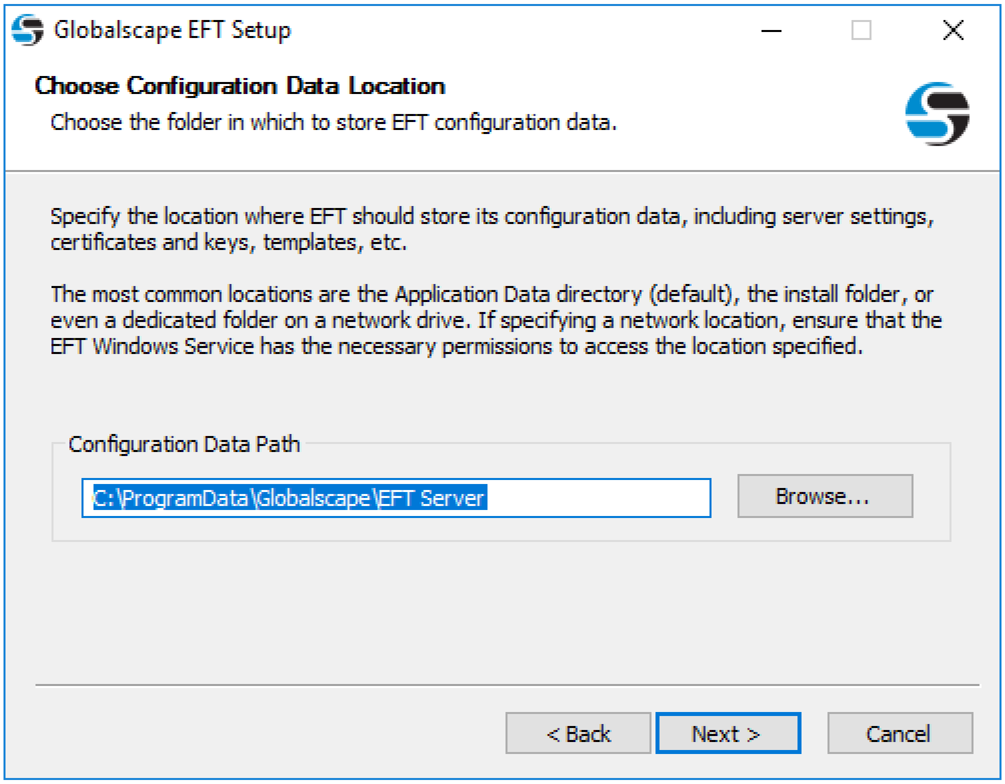
Choose the folder in which to install Globalscape EFT.

Setup will install Globalscape EFT in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\Program Files (x86)\Globalscape\EFT Server

Space required: 590.7MB
Space available: 23.4GB

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.)



Choose Configuration Data Location

Choose the folder in which to store EFT configuration data.

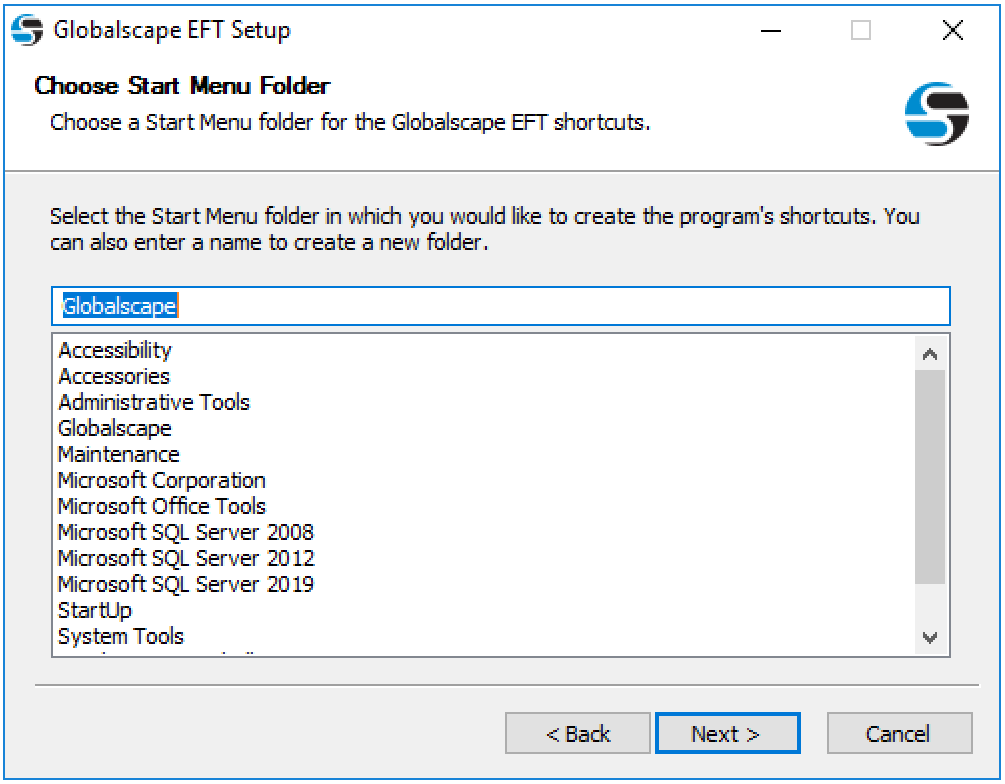
Specify the location where EFT should store its configuration data, including server settings, certificates and keys, templates, etc.

The most common locations are the Application Data directory (default), the install folder, or even a dedicated folder on a network drive. If specifying a network location, ensure that the EFT Windows Service has the necessary permissions to access the location specified.

Configuration Data Path

C:\ProgramData\Globalscape\EFT Server

8. Specify where you want to save EFT's 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.



Globalscape EFT Setup

Choose Start Menu Folder

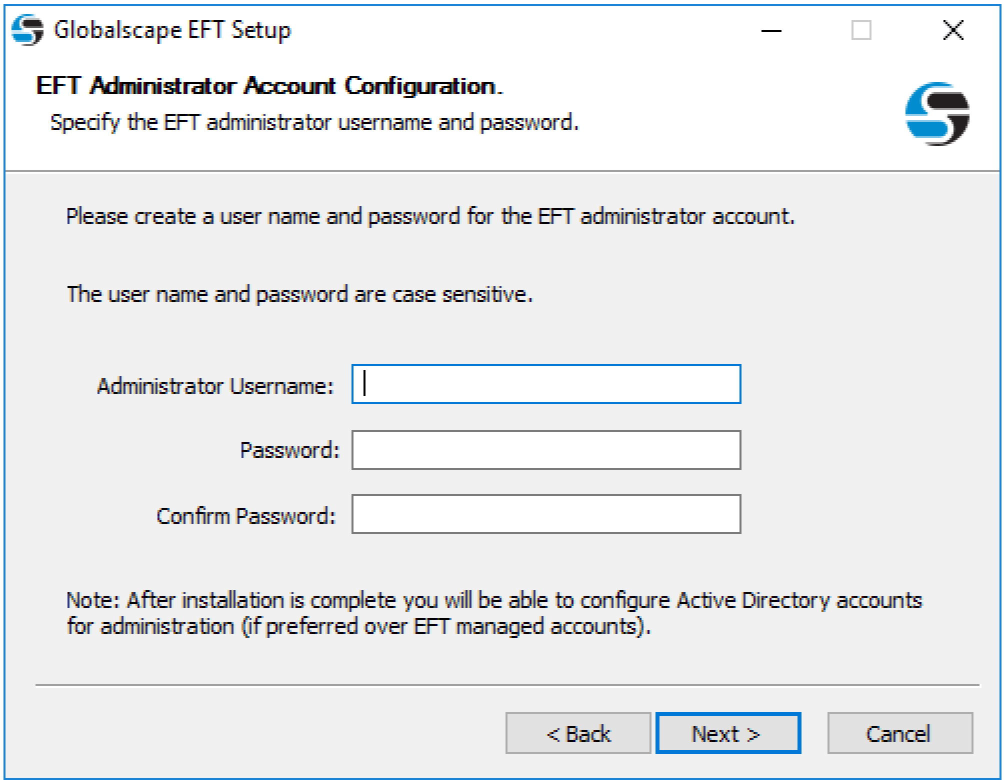
Choose a Start Menu folder for the Globalscape EFT shortcuts.

Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

Globalscape

Accessibility
Accessories
Administrative Tools
Globalscape
Maintenance
Microsoft Corporation
Microsoft Office Tools
Microsoft SQL Server 2008
Microsoft SQL Server 2012
Microsoft SQL Server 2019
StartUp
System Tools

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.



Globalscape EFT Setup

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:

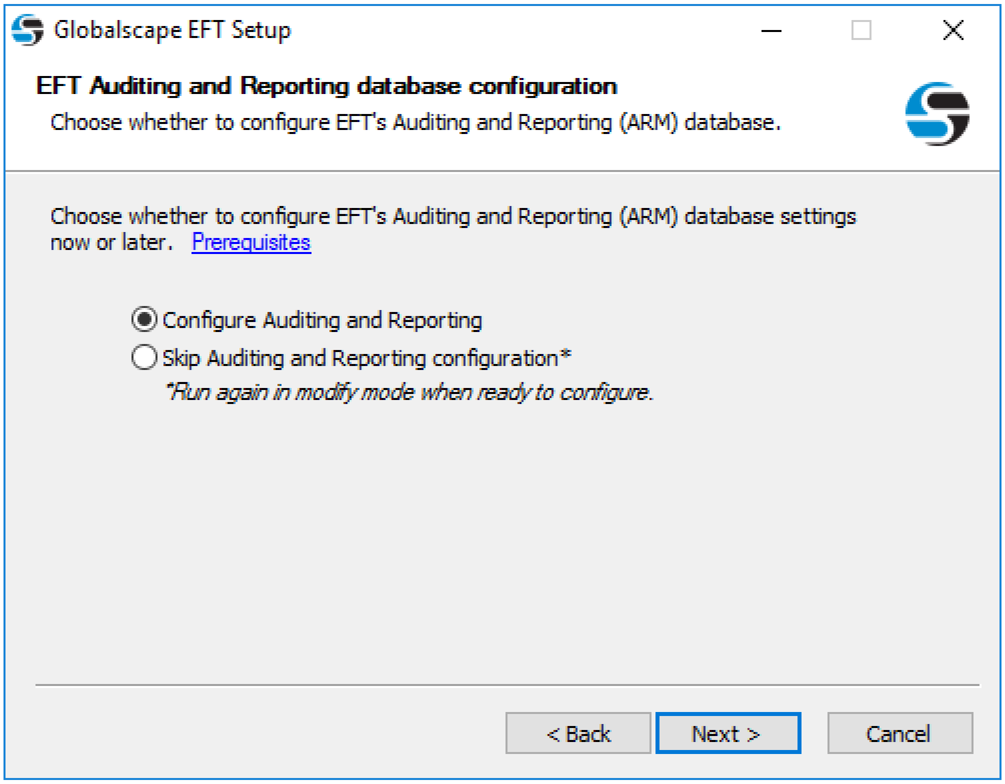
Confirm Password:

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

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.

    The administrator account password cannot be blank, can be up to 99 characters, and cannot be any of the following keywords: `password`, `administrator`, `administrator`, `sa`, or `sysadministrator`. 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.



Globalscape EFT Setup

EFT Auditing and Reporting database configuration

Choose whether to configure EFT's Auditing and Reporting (ARM) database.

Choose whether to configure EFT's Auditing and Reporting (ARM) database settings now or later. Prerequisites

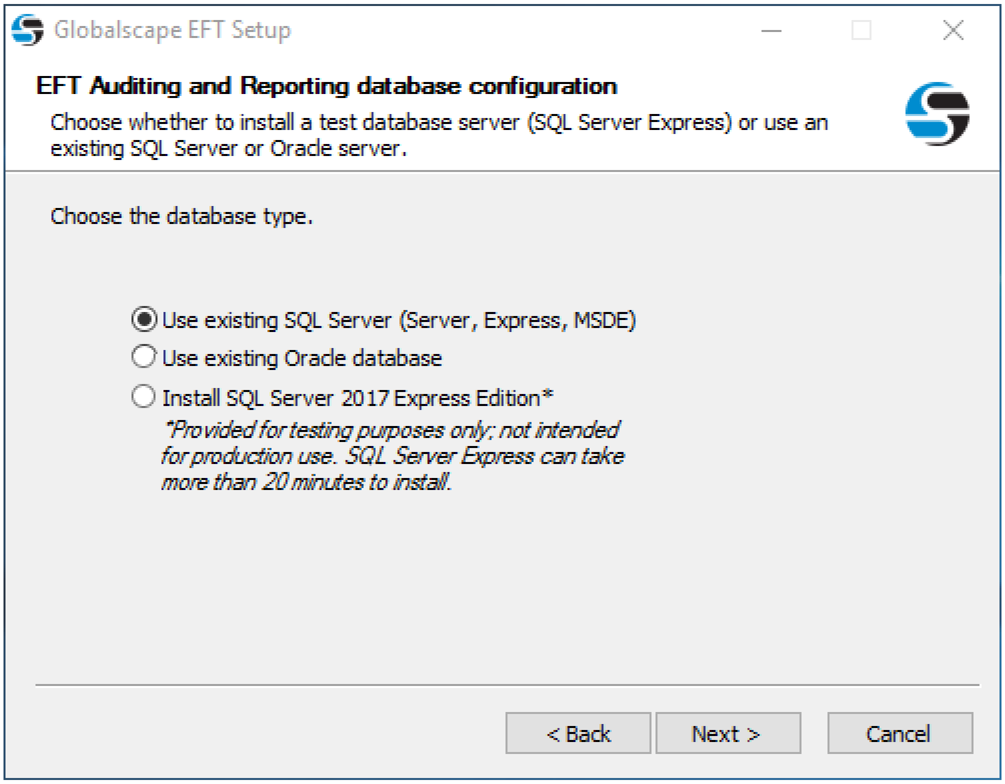
● Configure Auditing and Reporting

○ Skip Auditing and Reporting configuration*

**Run again in modify mode when ready to configure.*

- 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.)



EFT Auditing and Reporting database configuration

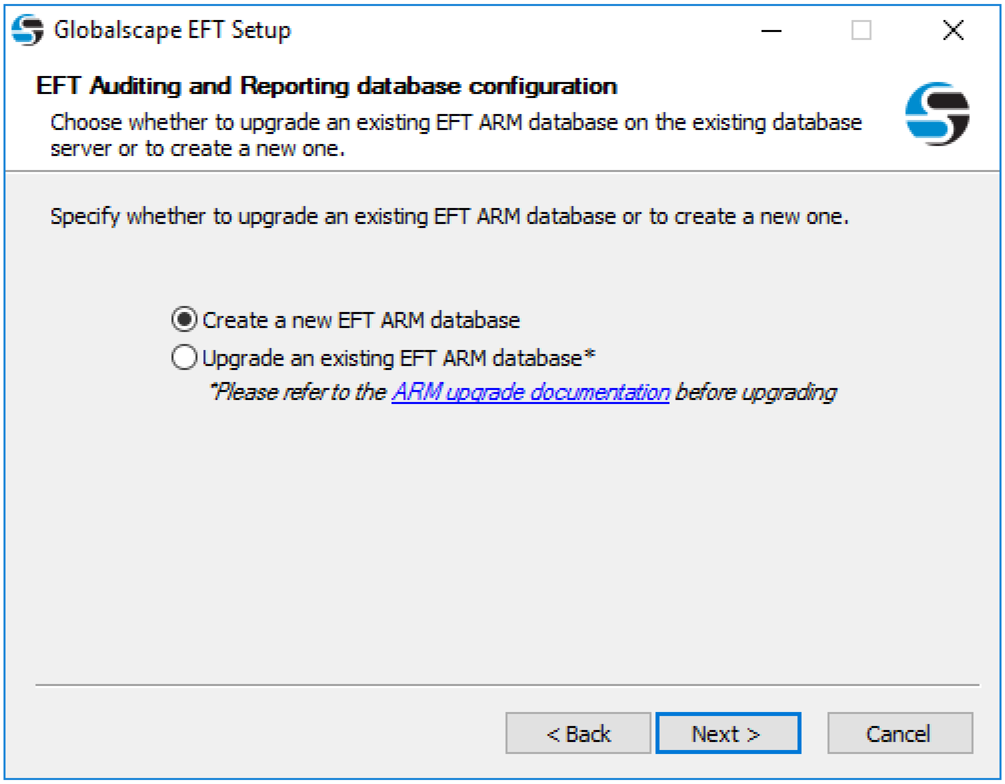
Choose whether to install a test database server (SQL Server Express) or use an existing SQL Server or Oracle server.

Choose the database type.

● Use existing SQL Server (Server, Express, MSDE)
○ Use existing Oracle database
○ Install SQL Server 2017 Express Edition*

**Provided for testing purposes only; not intended for production use. SQL Server Express can take more than 20 minutes to install.*

- **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:**



Globalscape EFT Setup

EFT 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.

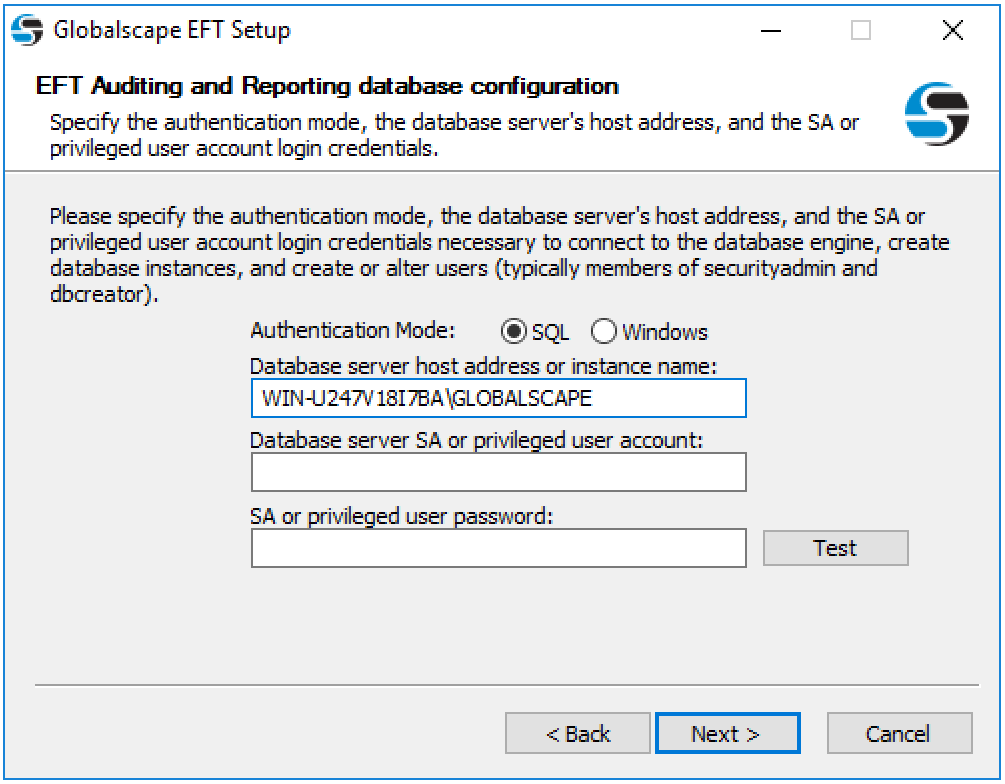
Specify whether to upgrade an existing EFT ARM database or to create a new one.

● Create a new EFT ARM database

○ Upgrade an existing EFT ARM database*

**Please refer to the ARM upgrade documentation before upgrading*

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



Globalscape EFT Setup

EFT Auditing and Reporting database configuration

Specify the authentication mode, the database server's host address, and the SA or privileged user account login credentials.

Please specify the authentication mode, the database server's host address, and the SA or privileged user account login credentials necessary to connect to the database engine, create database instances, and create or alter users (typically members of securityadmin and dbcreator).

Authentication Mode: ● SQL ○ Windows

Database server host address or instance name: WIN-U247V18I7BA\GLOBALSCAPE

Database server SA or privileged user account:

SA or privileged user password:

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.

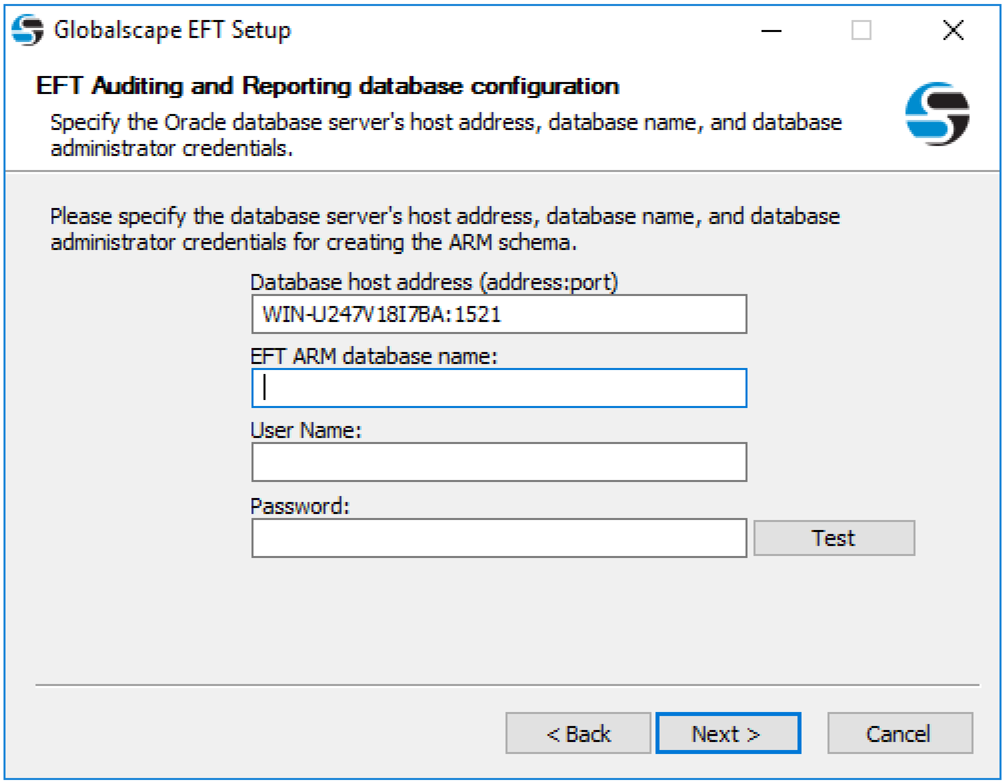
d. Specify the database server SA or privileged user account name (for example, sa).

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.



Globalscape EFT Setup

EFT Auditing and Reporting database configuration

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)
WIN-U247V18I7BA:1521

EFT ARM database name:

User Name:

Password:

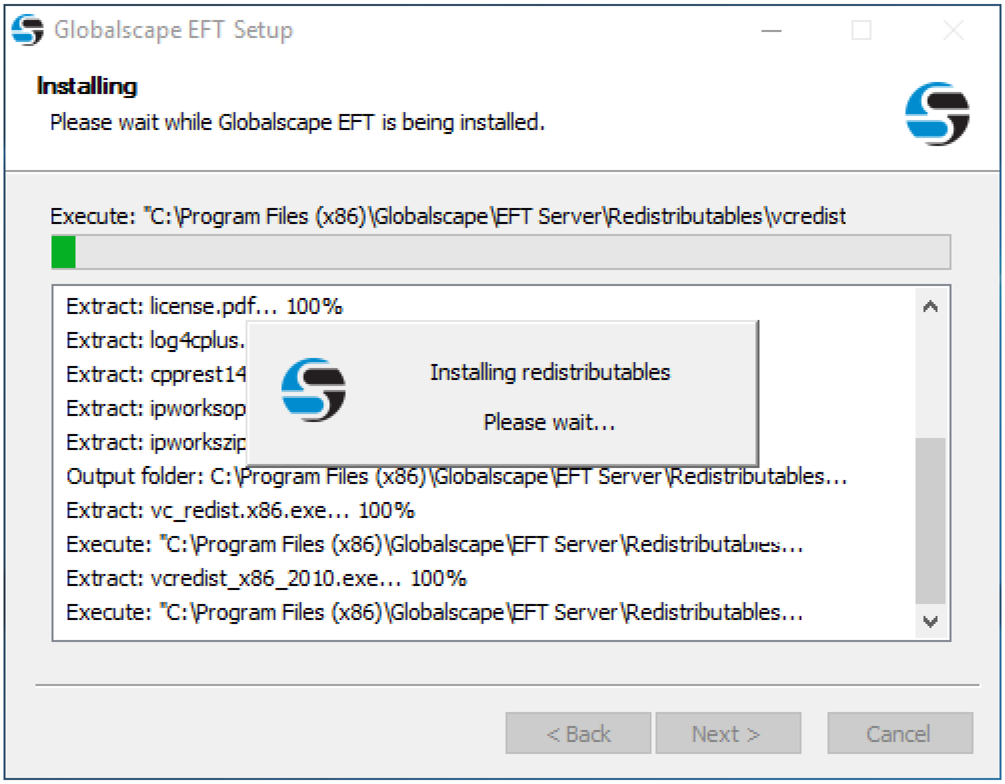
b. Specify the database host address and the EFT-specific schema name and database administrator credentials, and then click **Test** or **Next** to test the connection to the database. (If you have installed Oracle Database Express Edition (XE) for testing/demo purposes, the instance name is XE and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

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

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

16. Specify or create the ARM schema owner credentials, then click **Next**.

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

    Installing

    Please wait while Globalscape EFT is being installed.

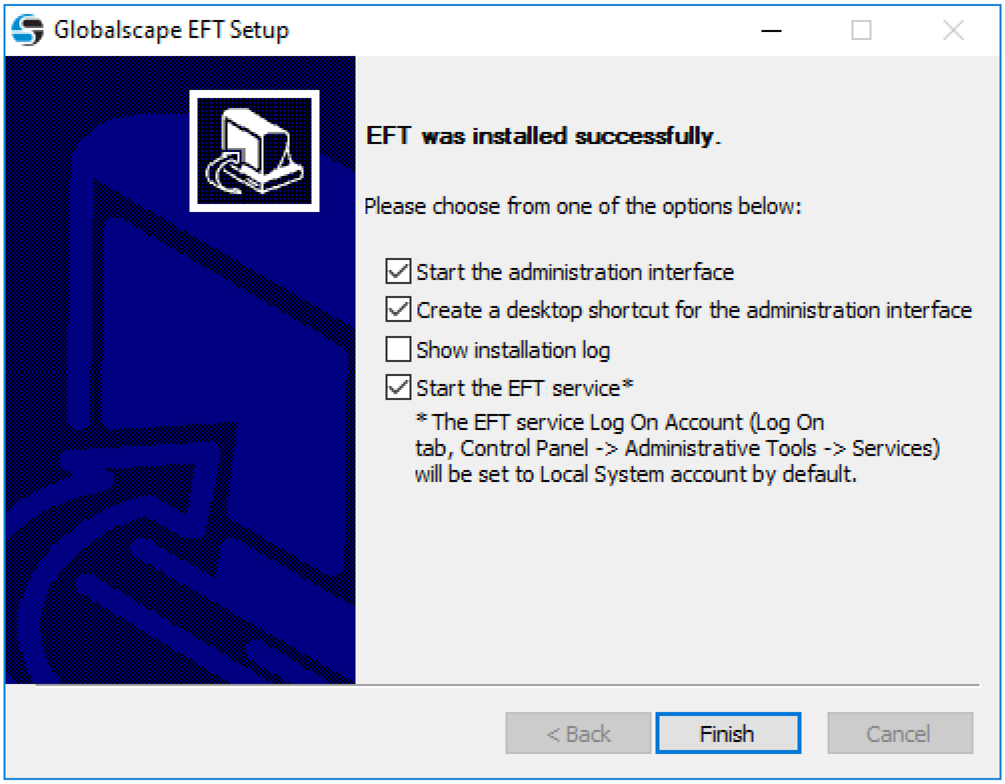
    Execute: "C:\Program Files (x86)\Globalscape\EFT Server\Redistributables\vcredist

    ```
    Extract: license.pdf... 100%
    Extract: log4cplus.
    Extract: cpprest14
    Extract: ipworksop
    Extract: ipworkszip
    Output folder: C:\Program Files (x86)\Globalscape\EFT Server\Redistributables...
    Extract: vc_redist.x86.exe... 100%
    Execute: "C:\Program Files (x86)\Globalscape\EFT Server\Redistributables...
    Extract: vcredist_x86_2010.exe... 100%
    Execute: "C:\Program Files (x86)\Globalscape\EFT Server\Redistributables...
    ```

    Installing redistributables

    Please wait...

17. 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.



EFT was installed successfully.

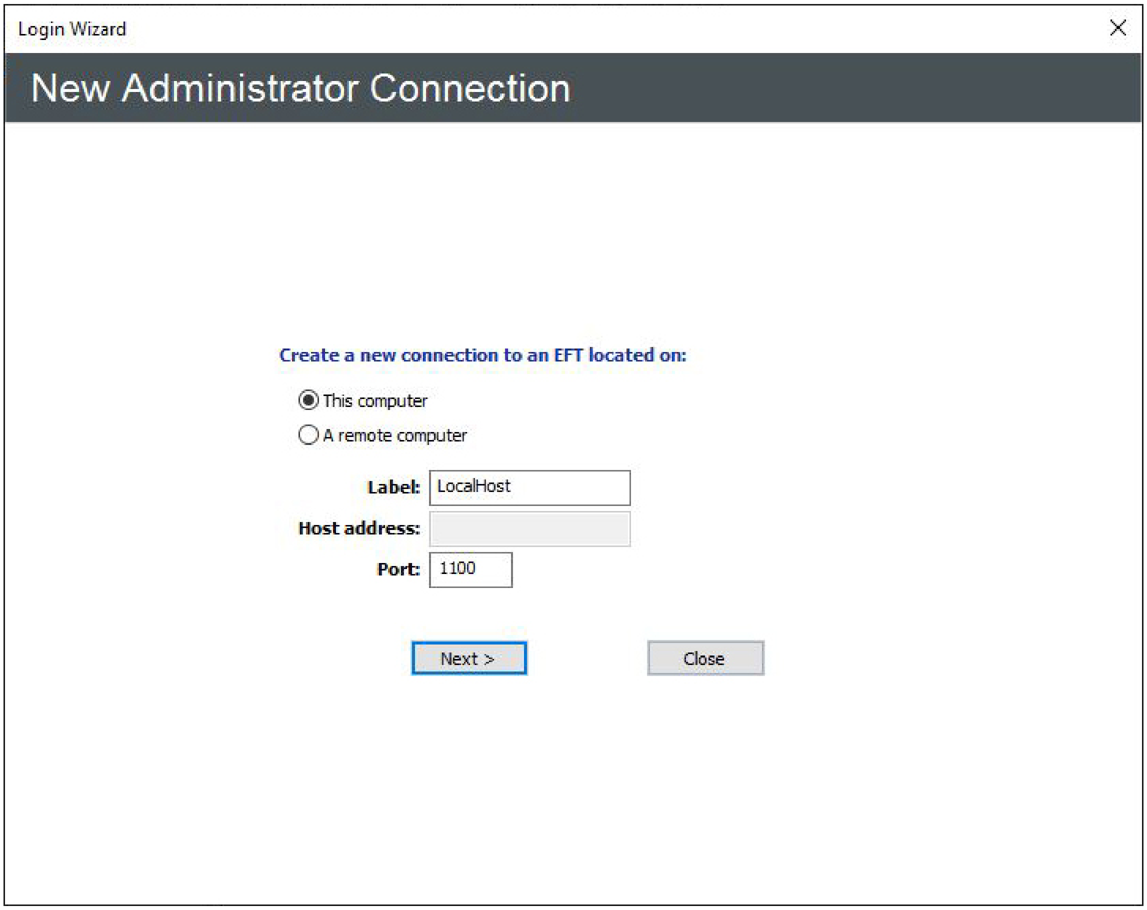
Please choose from one of the options below:

☑ Start the administration interface
☑ Create a desktop shortcut for the administration interface
□ Show installation log
☑ Start the EFT service*

* The EFT service Log On Account (Log On tab, Control Panel -> Administrative Tools -> Services) will be set to Local System account by default.

- **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."

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



Login Wizard

New Administrator Connection

Create a new connection to an EFT located on:

● This computer

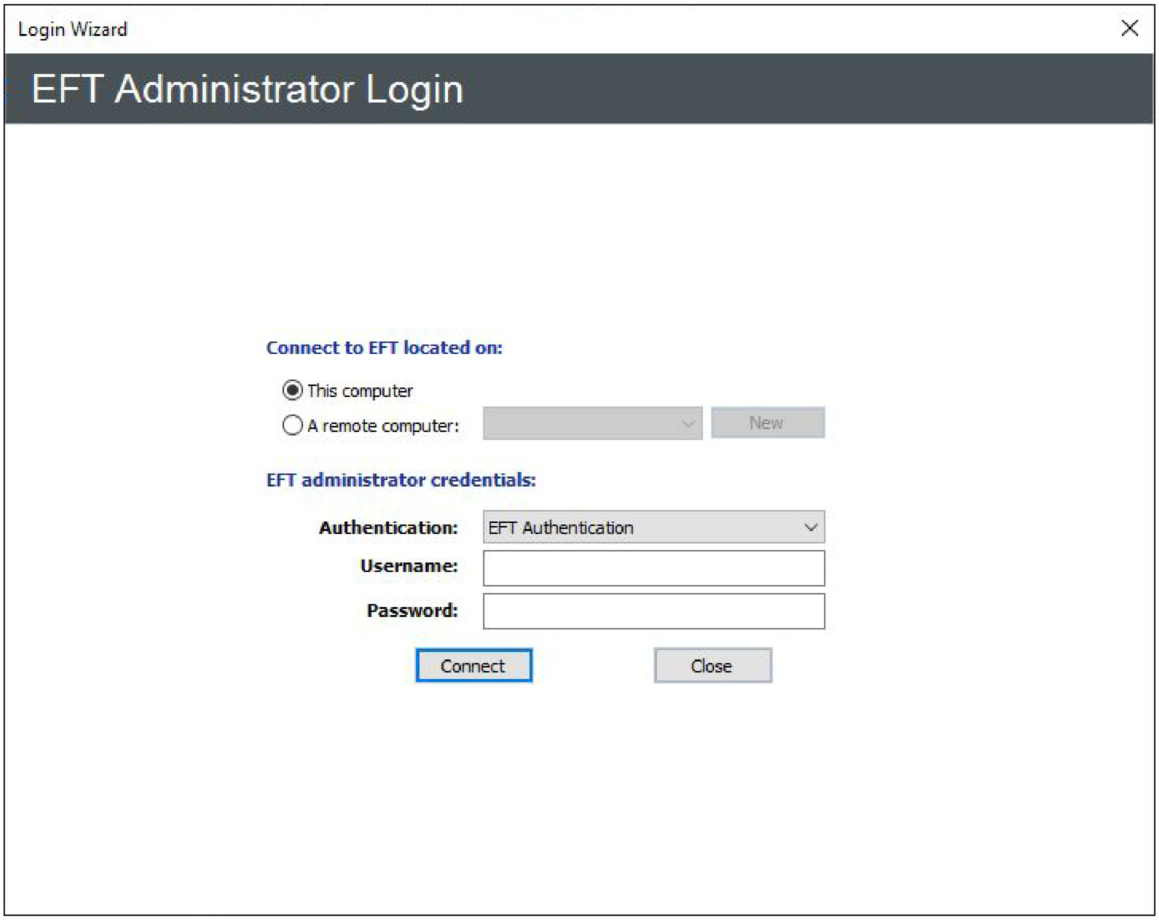
○ A remote computer

Label: LocalHost

Host address:

Port: 1100

19. 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.



Login Wizard

EFT Administrator Login

Connect to EFT located on:

● This computer

○ A remote computer:

EFT administrator credentials:

Authentication: EFT Authentication

Username:

Password:

20. 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.

21. 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.

Silent Command-Line Installation

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

Refer to https://help.globalscape.com/help/eft8-0/SilentInstallation.pdf for details.

> **NOTE:** If you install EFT HA via the silent installer, then, once configured, if you upgrade EFT via the install wizard, EFT fails to start the server service. The install wizard is setting the EFT server configuration details to the default paths. This issue only occurs when you use the silent installer for the initial deployment, then follow with an upgrade using the wizard. If you use the wizard for both installing and upgrading, or the silent installer for both installing and upgrading, this issue does not occur. Refer to https://kb.globalscape.com/Knowledgebase/11194/Upgrading-EFT-v7x-and-later for more information about upgrading.

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 (x86)\Globalscape\EFT Server** folder. It does not uninstall configuration files, Oracle or SQL Server tables, Reports, or Backup files.
- Your license information remains in the Windows Registry, in case you decide to reinstall.
- For HA installations, there will be configuration and EFT user files in the shared location.

Artifact Type	Artifact Default Location	Description
Database tables	ARM database; ODBC Authentication (SQL Server or Oracle)	Database-specific purge scripts are installed with EFT. The scripts are installed under the "SQL Server" and "Oracle" sub-directories of the **\ProgramData\Globalscape\EFT Server\ directory.**
Folder\Files	\Program Files (x86)\Common Files\Globalscape	Directory where application is installed
Folder\Files	\ProgramData\AutoMate	Directory where Advanced Workflow Engine files are installed
Folder\Files	\ProgramData\Globalscape	Directory where application configuration and site information is stored
Folder\Files	\Users\<usernames>\AppData\Local\GlobalSCAPE\	administrator user files; delete if no longer needed
Folder\Files	\Users\<usernames>\AppData\Roaming\GlobalSCAPE\	administrator user files; delete if no longer needed
Folder\Files	\inetpub\EFTRoot	EFT user files; delete if no longer needed
Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Globalscape	You can delete the entire **Globalscape** folder (if you have no other Globalscape products)
Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GlobalSCAPE Inc	You can delete the entire **Globalscape Inc** folder (if you have no other Globalscape products)
Registry	HKEY_CURRENT_USER\Software\Globalscape	You can delete the entire **Globalscape** folder (if you have no other Globalscape products)

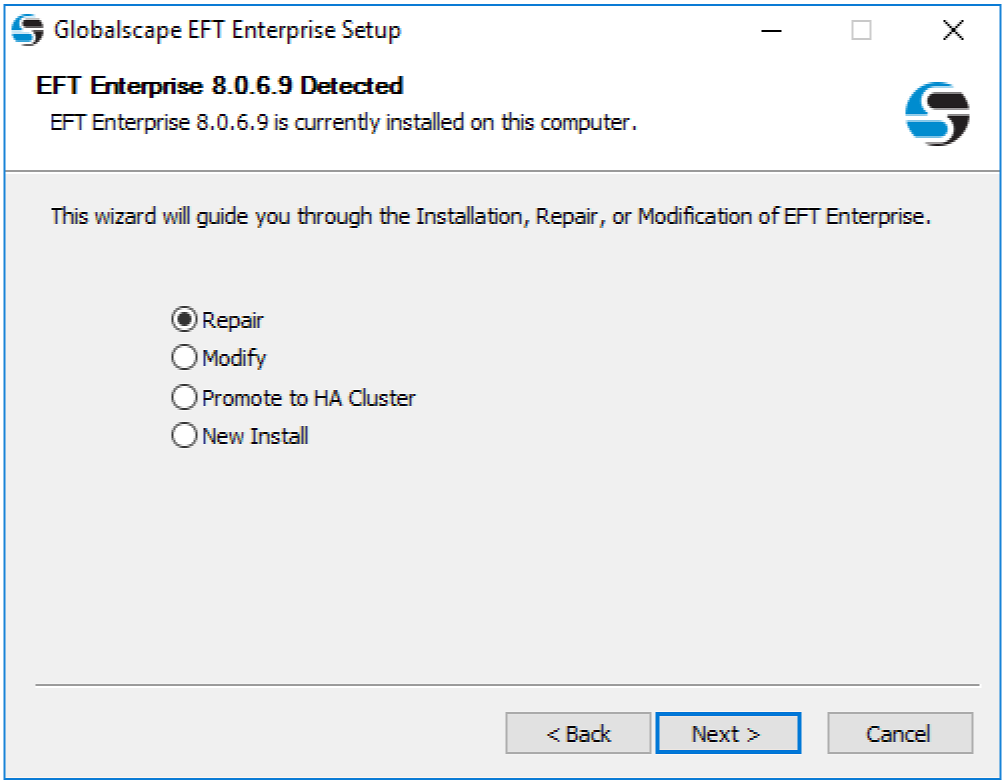
Artifact Type	Artifact Default Location	Description
Registry	HKEY_LOCAL_ MACHINE\SOFTWARE\Wow6432Node\Network Automation	AWE files; You can delete the entire **Network Automation** folder
TEMP folders	Temp location of account used for EFT service and Temp location of user running EFT installer	temporary files

Related Topics

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.


Globalscape EFT Enterprise Setup

EFT Enterprise 8.0.6.9 Detected

EFT Enterprise 8.0.6.9 is currently installed on this computer.

This wizard will guide you through the Installation, Repair, or Modification of EFT Enterprise.

● Repair
○ Modify
○ Promote to HA Cluster
○ New Install

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.

After You Are Done

Congratulations! EFT is now installed. Read the following topics for additional information and your next steps.

- Review Configuration and Security Best Practice for EFT Best Practices topics for helpful configuration tips and recommended settings
- Have your license key available
- Creating and Configuring an EFT Server
- Activating the Software (EFT and Modules)
- Windows Account for the EFT Service

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) before creating Servers and Sites. 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.

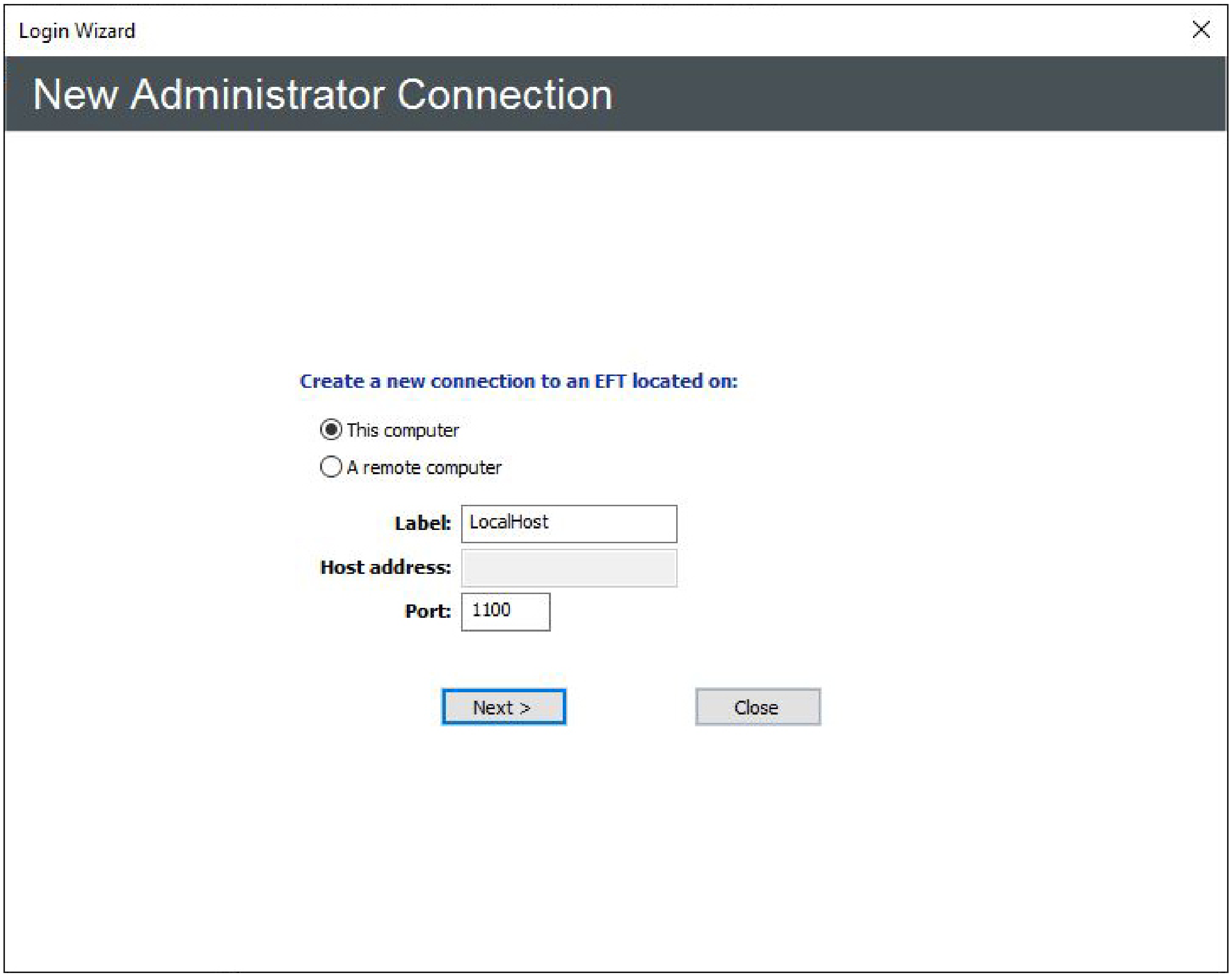
If you are configuring your first EFT Server connection, refer to **Configure the First EFT Connection**, below. If you are configuring a new, remote EFT connection, refer to **Creating a Remote Connection**.

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**.)



Login Wizard

New Administrator Connection

Create a new connection to an EFT located on:

● This computer

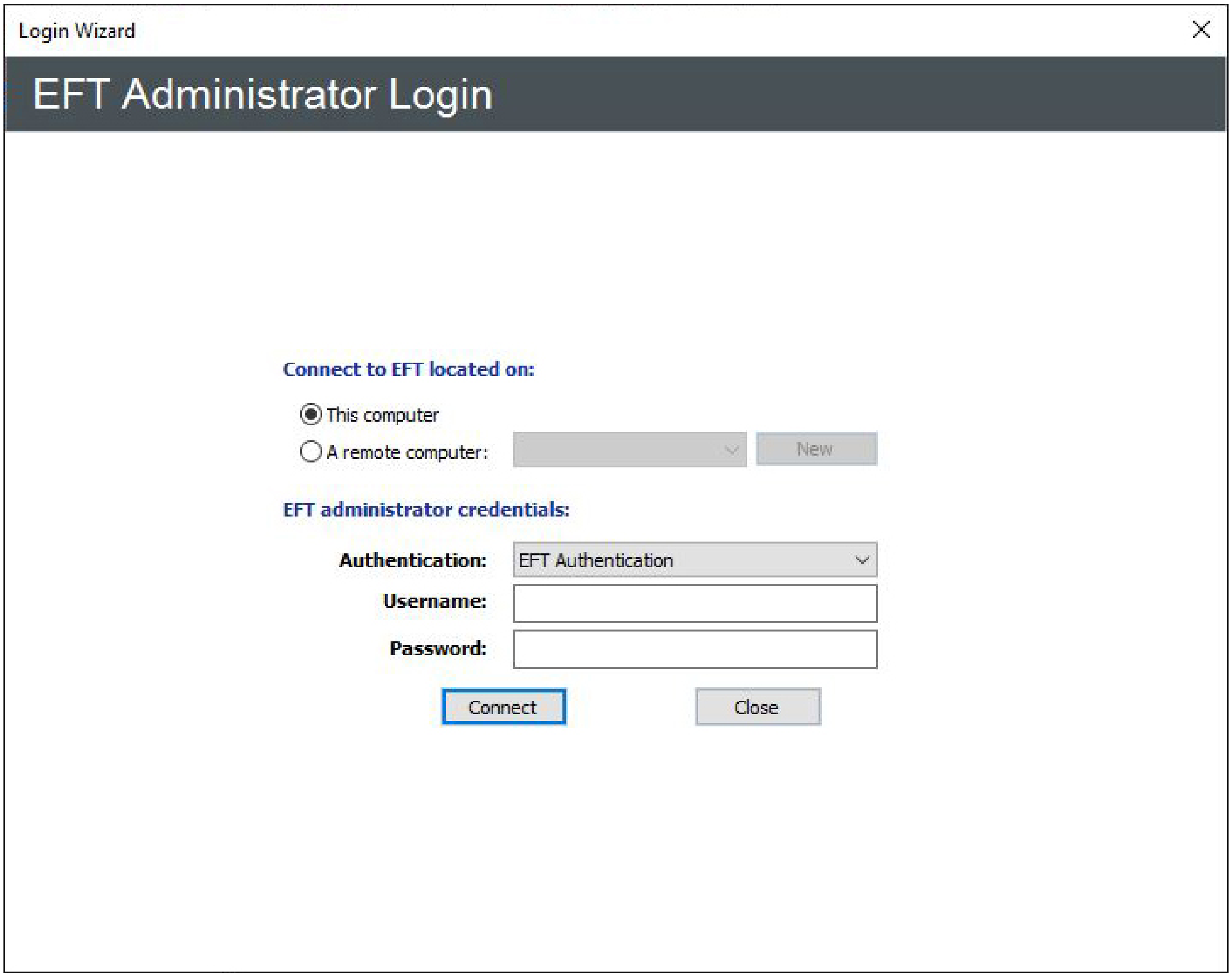
○ A remote computer

Label: LocalHost

Host address:

Port: 1100

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.



Login Wizard

EFT Administrator Login

Connect to EFT located on:

● This computer

○ A remote computer:

EFT administrator credentials:

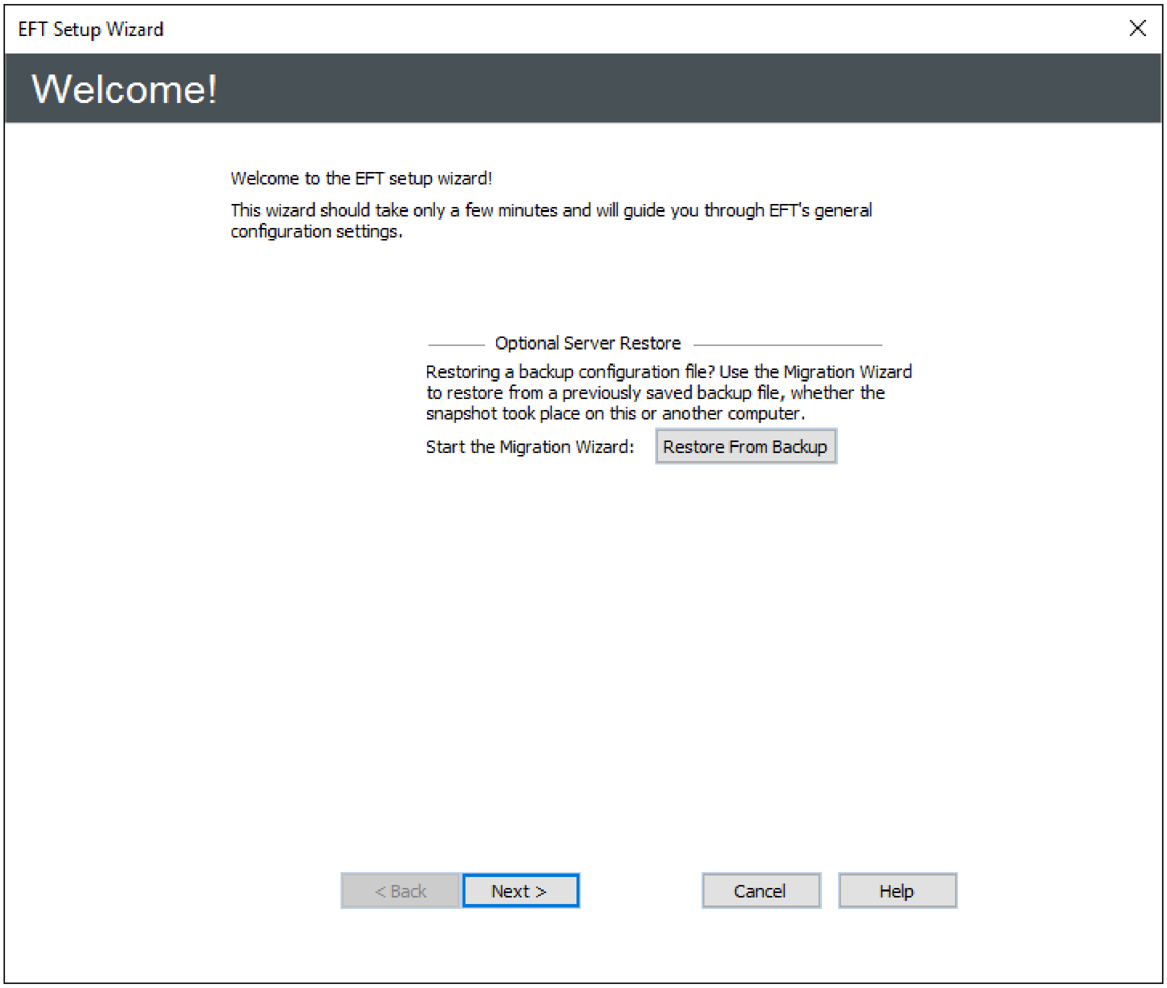
Authentication: EFT Authentication

Username:

Password:

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.
4. Click **Next**. The **Server Setup** wizard **Welcome** page appears.



EFT Setup Wizard

Welcome!

Welcome to the EFT setup wizard!

This wizard should take only a few minutes and will guide you through EFT's general configuration settings.

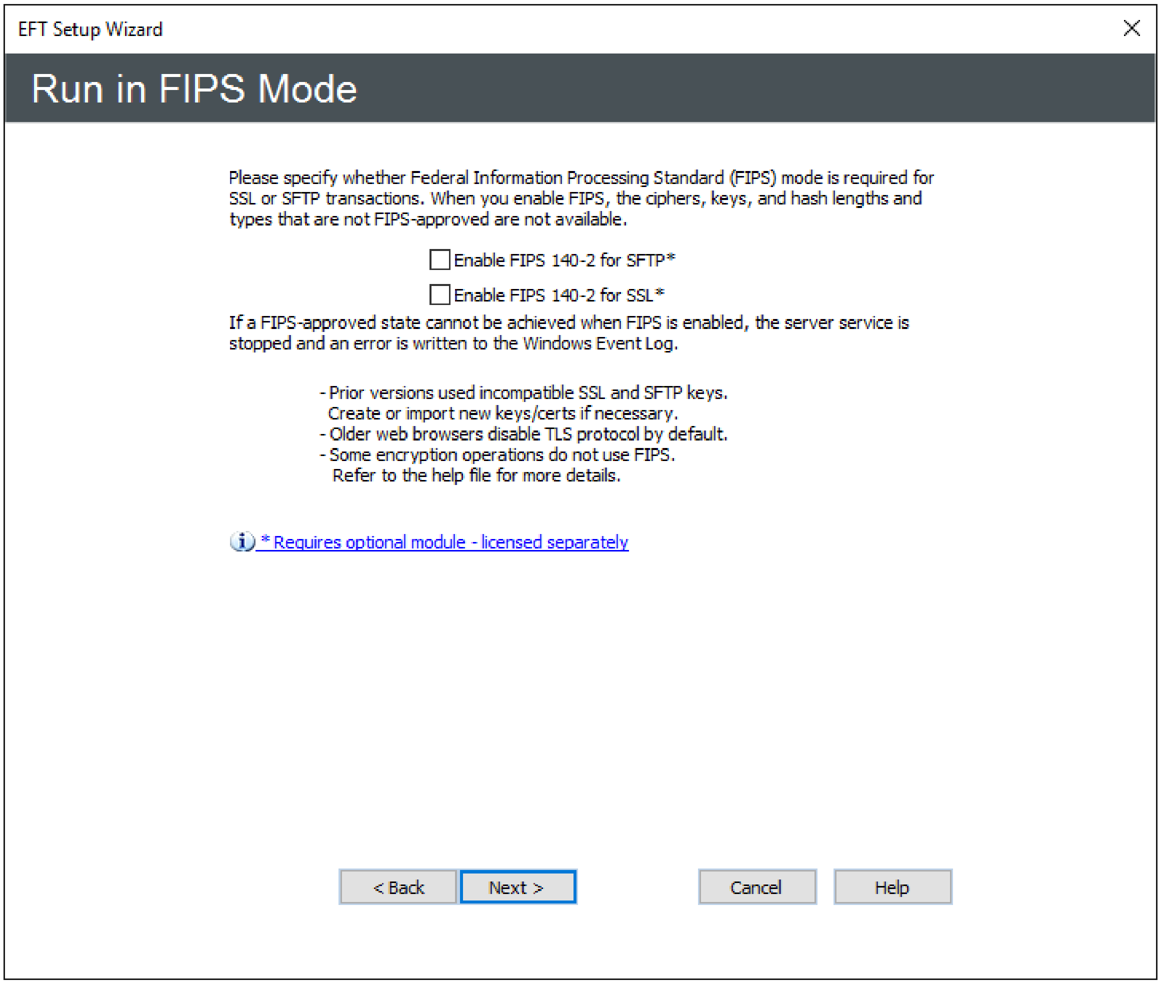
Optional Server Restore

Restoring a backup configuration file? Use the Migration Wizard to restore from a previously saved backup file, whether the snapshot took place on this or another computer.

Start the Migration Wizard: Restore From Backup

- 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.

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



EFT Setup Wizard

Run in FIPS Mode

Please specify whether Federal Information Processing Standard (FIPS) mode is required for SSL or SFTP transactions. When you enable FIPS, the ciphers, keys, and hash lengths and types that are not FIPS-approved are not available.

□ Enable FIPS 140-2 for SFTP*

□ Enable FIPS 140-2 for SSL*

If a FIPS-approved state cannot be achieved when FIPS is enabled, the server service is stopped and an error is written to the Windows Event Log.

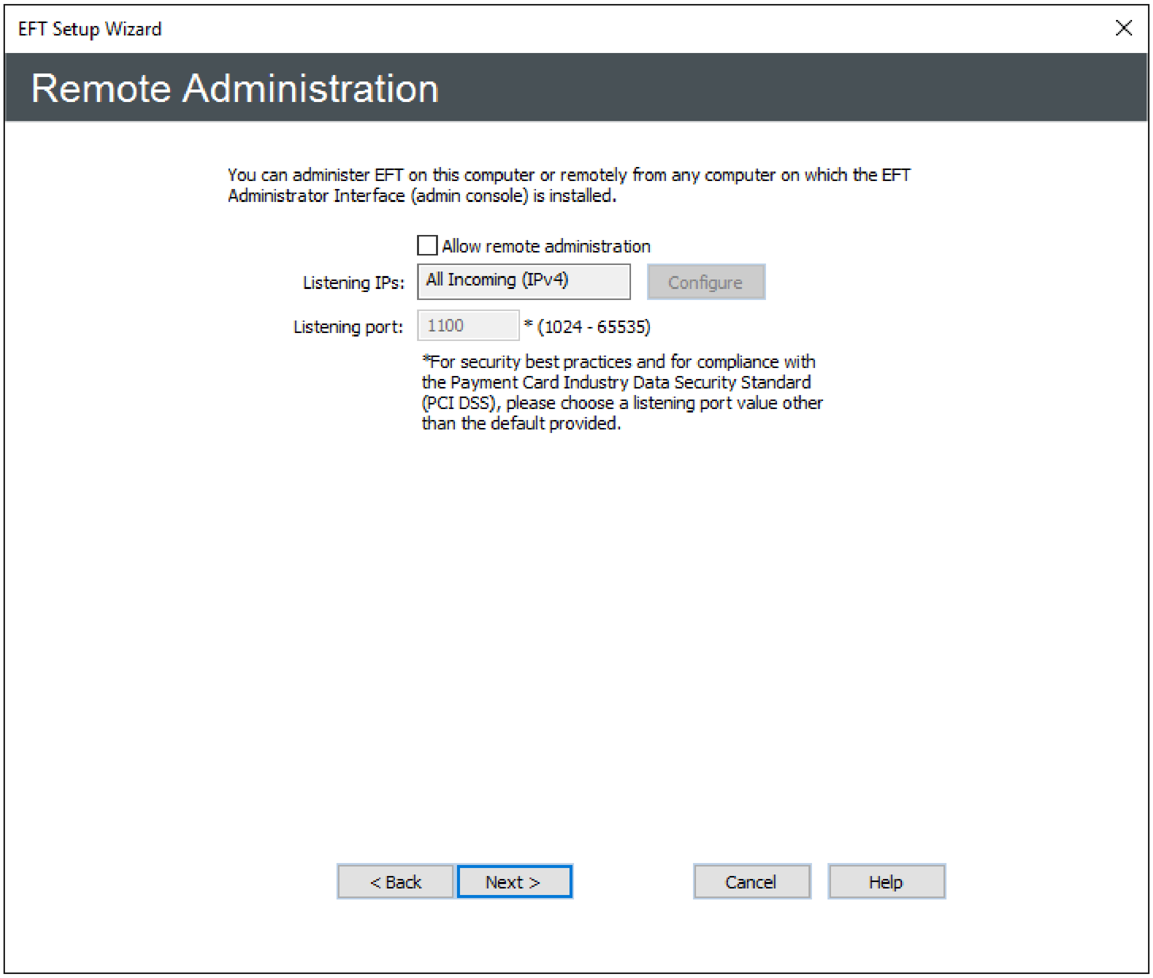
- Prior versions used incompatible SSL and SFTP keys.
  Create or import new keys/certs if necessary.
- Older web browsers disable TLS protocol by default.
- Some encryption operations do not use FIPS.
  Refer to the help file for more details.

* Requires optional module - licensed separately

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.

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


EFT Setup Wizard

Remote Administration

You can administer EFT on this computer or remotely from any computer on which the EFT Administrator Interface (admin console) is installed.

□ Allow remote administration

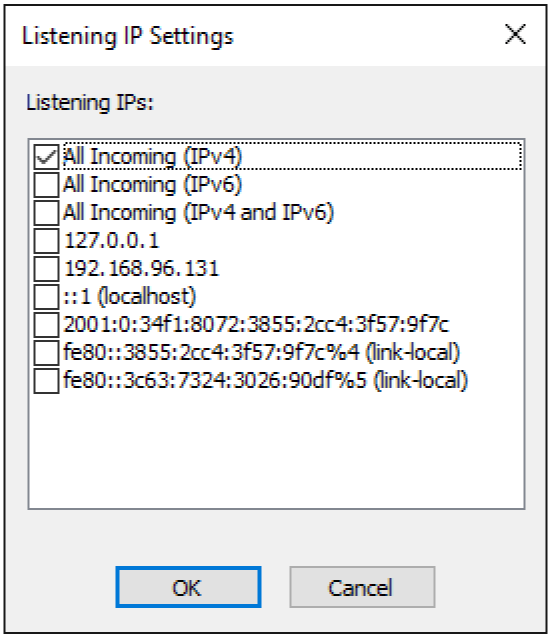
Listening IPs: All Incoming (IPv4)

Listening port: 1100 * (1024 - 65535)

*For security best practices and for compliance with the Payment Card Industry Data Security Standard (PCI DSS), please choose a listening port value other than the default provided.

- 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.



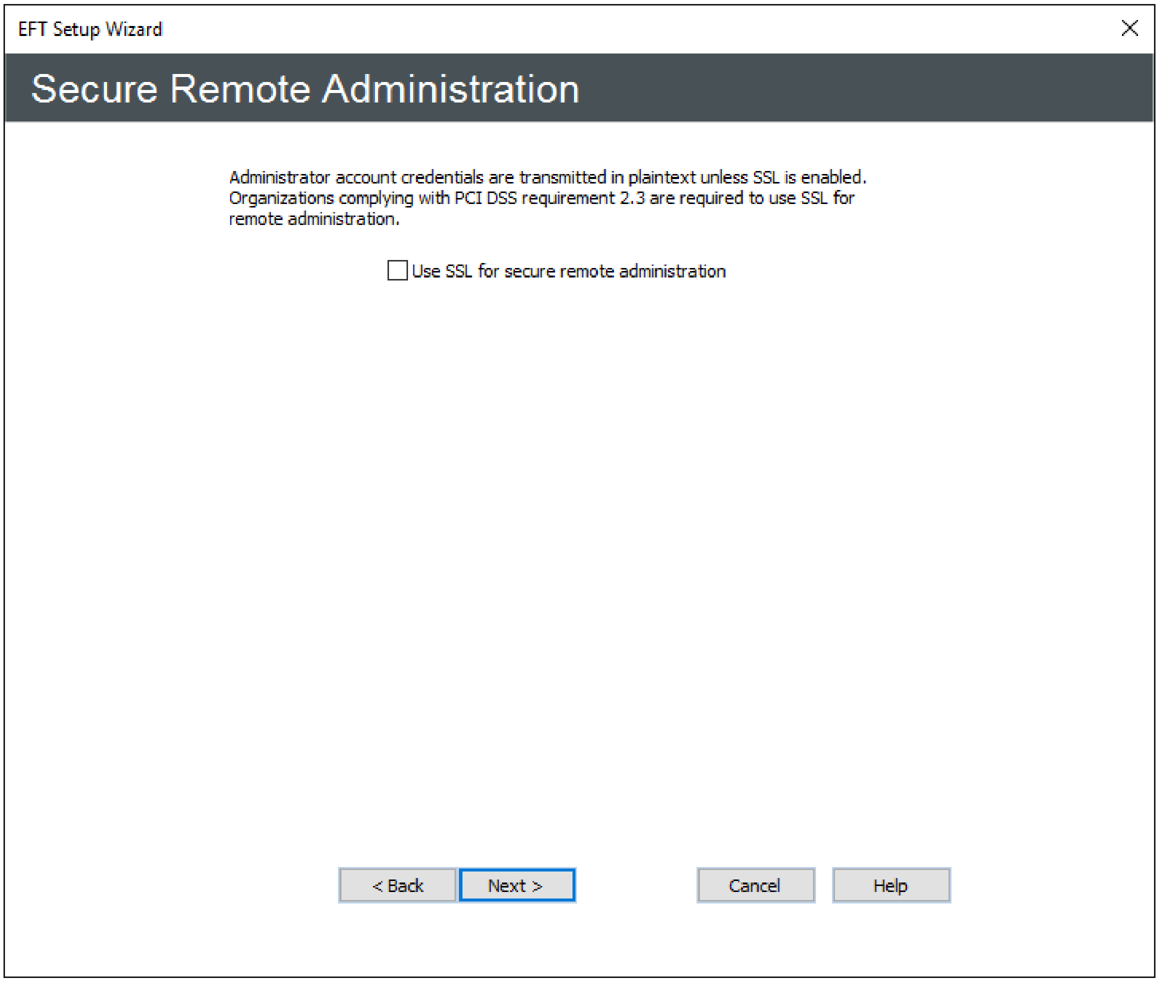
Listening IP Settings

Listening IPs:

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

- **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**.

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



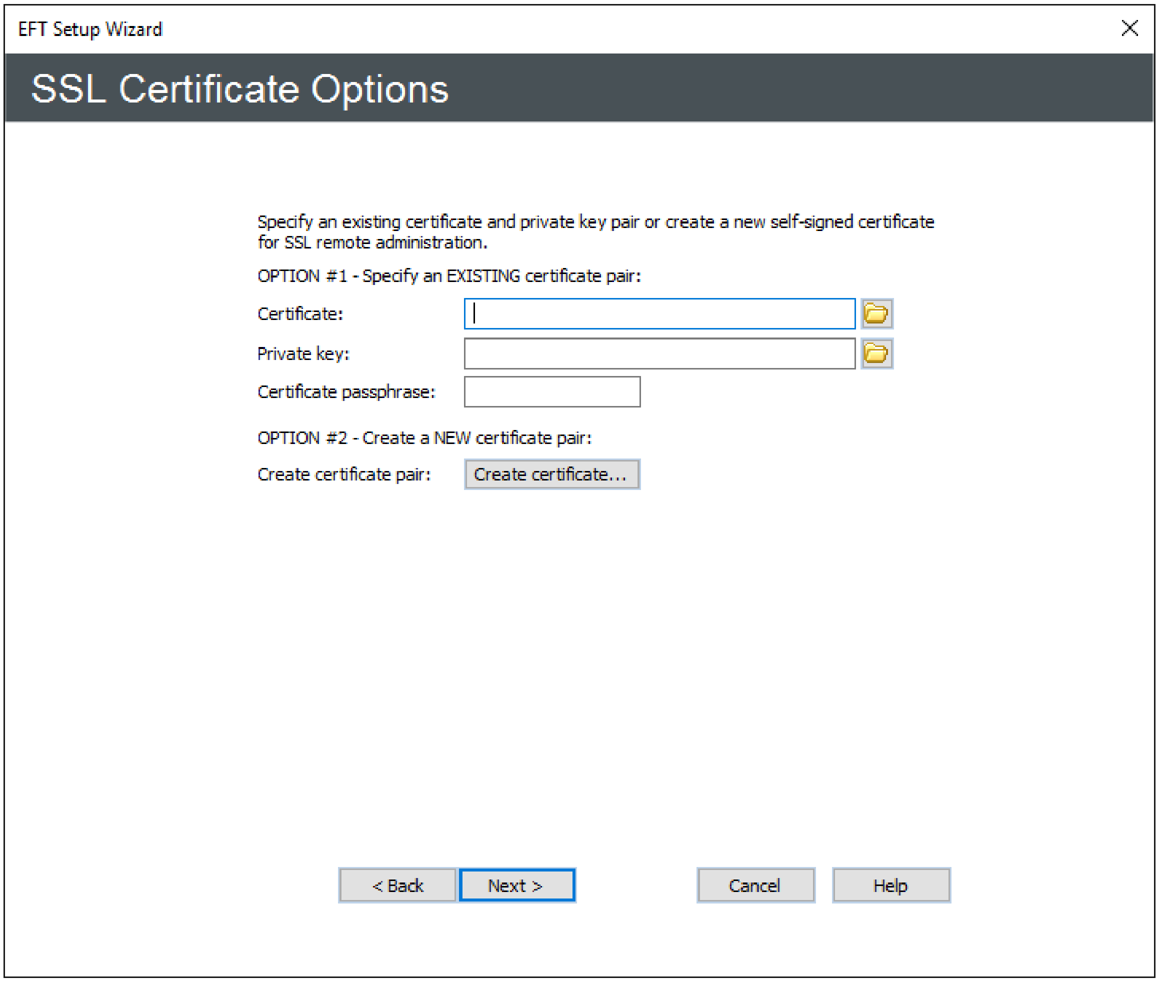
EFT Setup Wizard

Secure Remote Administration

Administrator account credentials are transmitted in plaintext unless SSL is enabled. Organizations complying with PCI DSS requirement 2.3 are required to use SSL for remote administration.

☐ Use SSL for secure remote administration

9. 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.



EFT Setup Wizard

SSL Certificate Options

Specify an existing certificate and private key pair or create a new self-signed certificate for SSL remote administration.

OPTION #1 - Specify an EXISTING certificate pair:

Certificate:

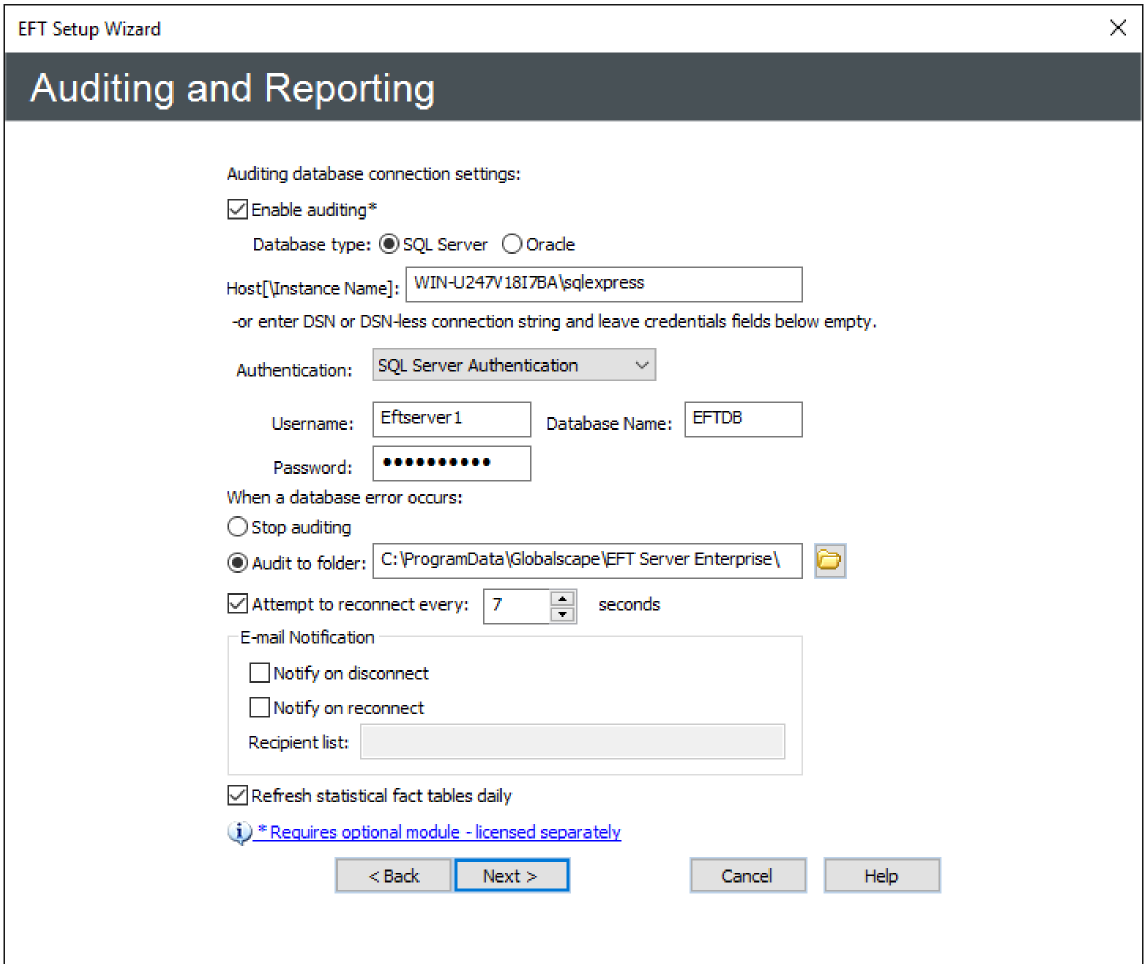
Private key:

Certificate passphrase:

OPTION #2 - Create a NEW certificate pair:

Create certificate pair:

10. 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.
11. Click **Next**. The **Auditing and Reporting** page appears.



EFT Setup Wizard

Auditing and Reporting

Auditing database connection settings:

☑ Enable auditing*

Database type: ● SQL Server ○ Oracle

Host[\Instance Name]: WIN-U247V18I7BA\sqlexpress

-or enter DSN or DSN-less connection string and leave credentials fields below empty.

Authentication: SQL Server Authentication

Username: Eftserver1 Database Name: EFTDB

Password: •••••••••••

When a database error occurs:

○ Stop auditing

● Audit to folder: C:\ProgramData\Globalscape\EFT Server Enterprise\

☑ Attempt to reconnect every: 7 seconds

E-mail Notification

☐ Notify on disconnect

☐ Notify on reconnect

Recipient list:

☑ Refresh statistical fact tables daily

* Requires optional module - licensed separately

12. 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**.

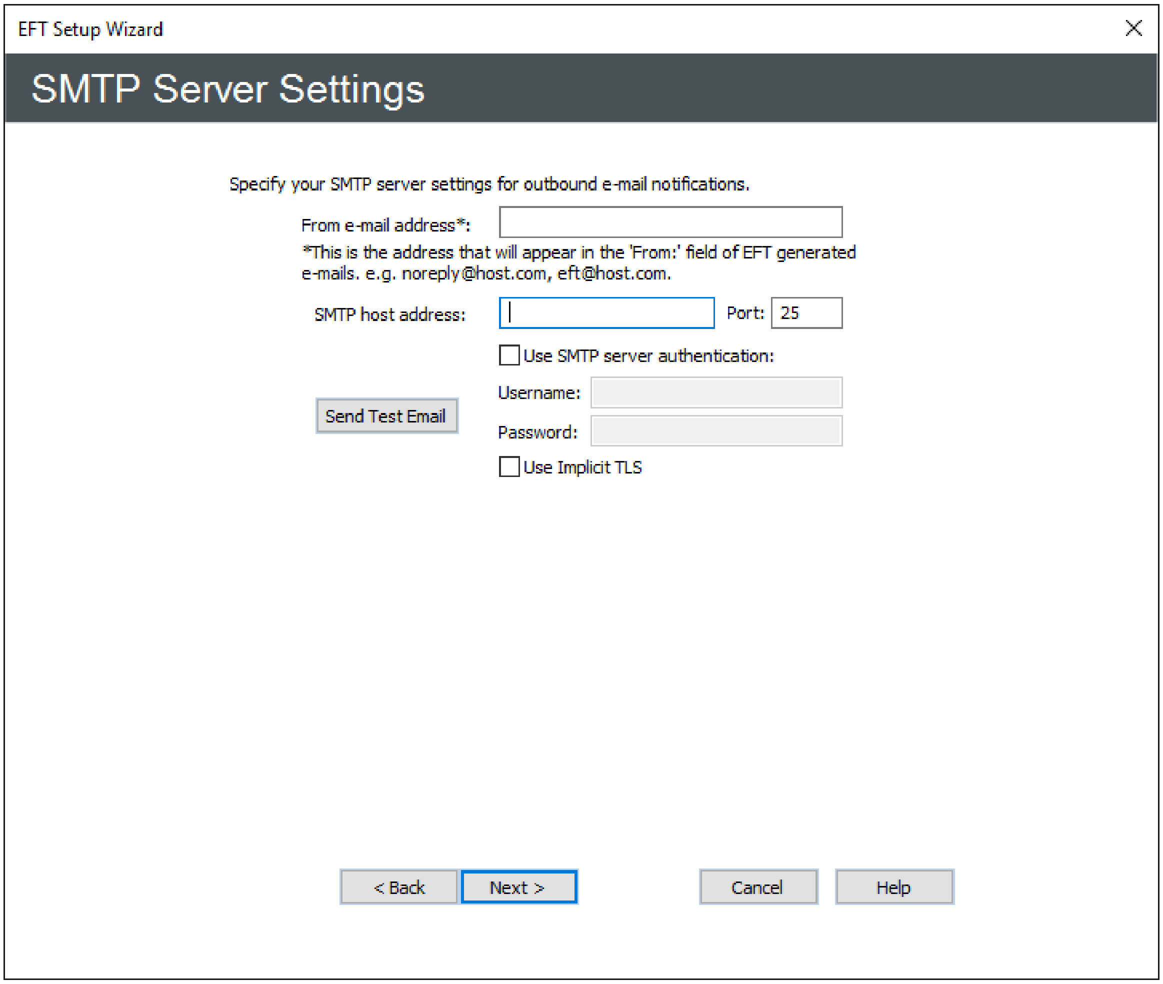
       - If you choose **SQL Server Authentication**, you must also specify the "sa" username and password. In the **Username** and **Password** boxes, type the username and password used to connect to the database (***not*** the EFT credentials).

    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.)

13. To try to recover from a database error automatically, select the **Attempt to reconnect every** check box and specify the frequency in seconds.
14. 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.
15. 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.
16. Click **Next**. The specify **SMTP Server Settings** page appears.



EFT Setup Wizard

SMTP Server Settings

Specify your SMTP server settings for outbound e-mail notifications.

From e-mail address*:

*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: Port: 25

□ Use SMTP server authentication:

Username:

Password:

□ Use Implicit TLS

17. In the **From email address** box, specify the email address for email notifications (such as those triggered by Event Rules). This is the address that appears in the From box of emails sent by EFT. For example, type `noreply@serverhost.com`.
    - The email address syntax is validated when you click **OK**. If the email address contains invalid characters or does not contain @, an error message appears. Click **OK** to dismiss the error message, then correct the address.
18. In the **SMTP host address** boxes, specify the SMTP server host address and port.
19. Select the **Use SMTP server authentication** check box, if needed, and provide the **Username** and **Password**.
    - Click **Send Test Email** to ensure the credentials are correct.
20. 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.

21. 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.

22. If you chose **Run the Site Setup wizard now**, the Site Setup wizard **Welcome** page appears.

23. Refer to Creating a Site for the procedure for configuring the Site. The procedure differs depending on the user authentication type you choose.

Configuration and Security Best Practices

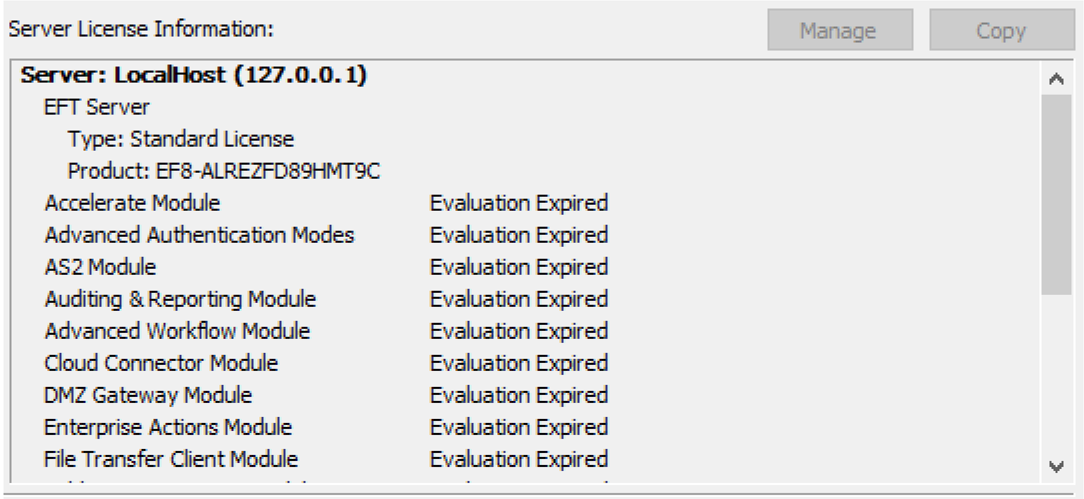
Refer to Globalscape Knowledgebase article #11312 for details about configuration and security best practices.

Activating the Software (EFT and Modules)

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 activate the EFT license (after a trial of a new installation, not an upgrade), the About EFT dialog box shows that EFT is licensed, but each of the modules has expired.



Server License Information:

Server: LocalHost (127.0.0.1)

EFT Server

Type: Standard License

Product: EF8-ALREZFD89HMT9C

Accelerate Module	Evaluation Expired
Advanced Authentication Modes	Evaluation Expired
AS2 Module	Evaluation Expired
Auditing & Reporting Module	Evaluation Expired
Advanced Workflow Module	Evaluation Expired
Cloud Connector Module	Evaluation Expired
DMZ Gateway Module	Evaluation Expired
Enterprise Actions Module	Evaluation Expired
File Transfer Client Module	Evaluation Expired

If the trial is not sufficient, you may be eligible to extend your trial. Contact your Globalscape account representative for more information.

When the trial period is over, no external IP addresses can connect to EFT, nor can EFT connect to any external IP addresses, until you enter a valid license.

For subscription licenses:

> IMPORTANT: When upgrading to v8.0.7, please register EFT "core" first before you register any module licenses.

- 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.
    - If there are additional years remaining in your term, EFT will successful renew and start its countdown to the next renewal date.
    - If your subscription has ran 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 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.

  Internet access is a pre-requisite to complete activation of a subscription license. 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.

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.

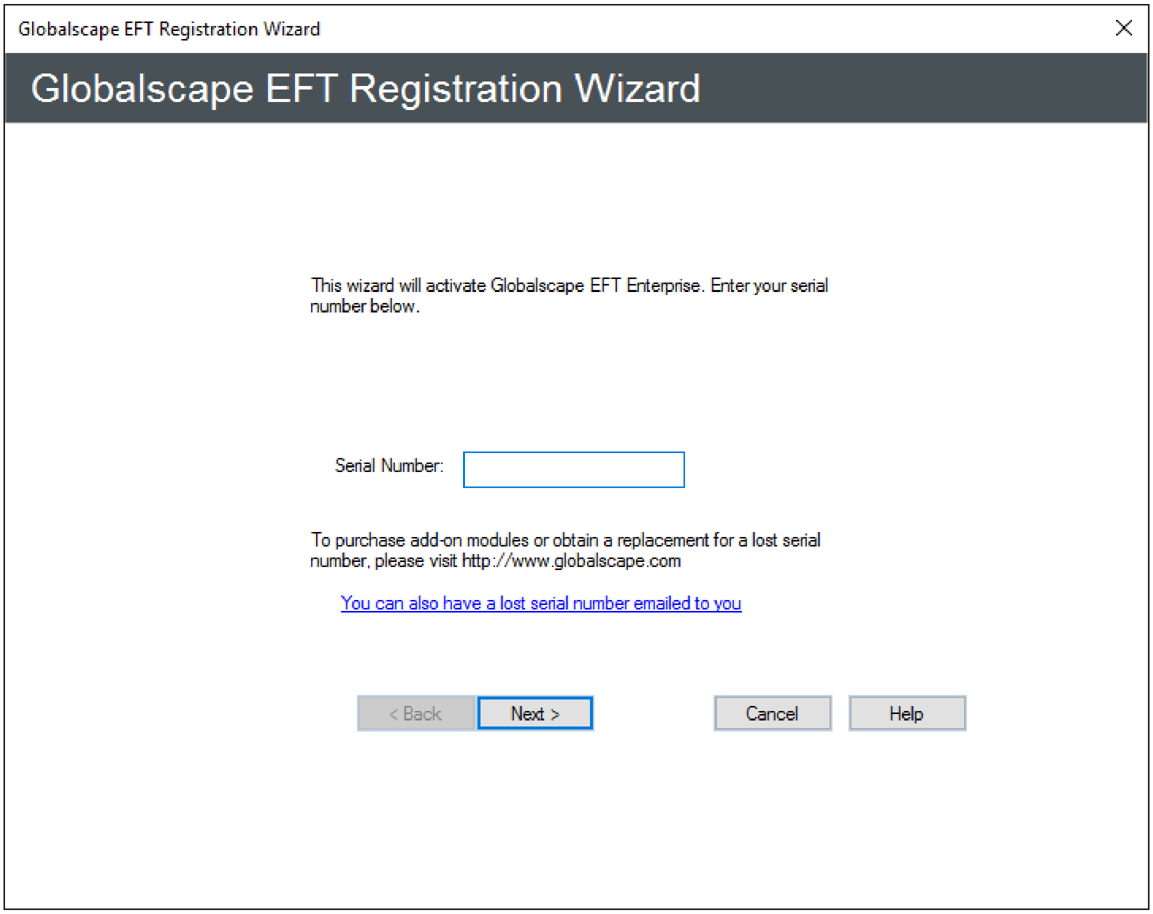
After you activate a product, the "Activate" text for that product on the **Help** menu is dimmed/unavailable.

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

1. Start the administration interface and provide your EFT administrator credentials (created at installation). The **Welcome** message appears.
2. Do one of the following:
    - Click **Enter Serial Number**. The **Registration Wizard** appears.

    - On the main menu click **Help**, and then click the product you want to activate.

   The **Registration Wizard** appears.



Globalscape EFT Registration Wizard
Globalscape EFT Registration Wizard

This wizard will activate Globalscape EFT Enterprise. Enter your serial number below.

Serial Number:

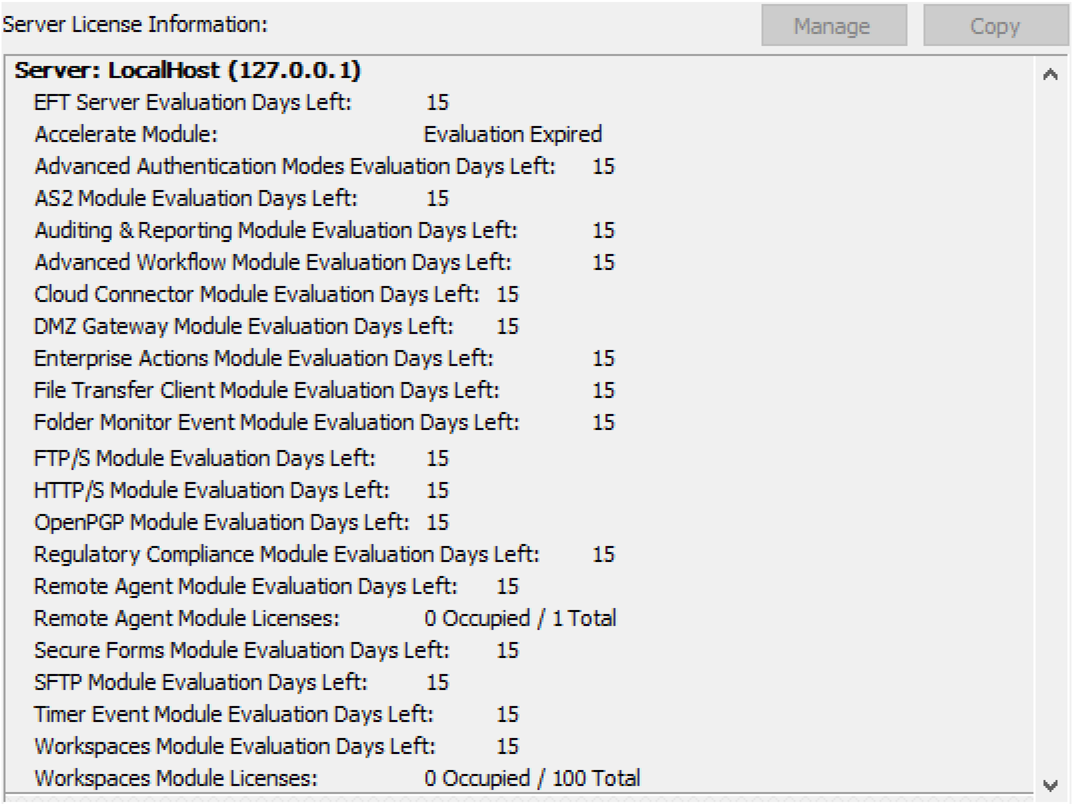
To purchase add-on modules or obtain a replacement for a lost serial number, please visit http://www.globalscape.com

You can also have a lost serial number emailed to you

< Back
Next >
Cancel
Help

3. In the **Serial Number** box, provide your serial number, and then click **Next**.
4. You should receive a message confirming online activation. Click **OK**. Activation is complete. (If registration fails, try entering your serial number again.)
5. 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.

Below is the license information that appears during trial mode before anything is activated.



```
Server License Information:

Server: LocalHost (127.0.0.1)
   EFT Server Evaluation Days Left:          15
   Accelerate Module:                        Evaluation Expired
   Advanced Authentication Modes Evaluation Days Left:      15
   AS2 Module Evaluation Days Left:          15
   Auditing & Reporting Module Evaluation Days Left:        15
   Advanced Workflow Module Evaluation Days Left:           15
   Cloud Connector Module Evaluation Days Left:  15
   DMZ Gateway Module Evaluation Days Left:      15
   Enterprise Actions Module Evaluation Days Left:          15
   File Transfer Client Module Evaluation Days Left:        15
   Folder Monitor Event Module Evaluation Days Left:        15
   FTP/S Module Evaluation Days Left:        15
   HTTP/S Module Evaluation Days Left:       15
   OpenPGP Module Evaluation Days Left:  15
   Regulatory Compliance Module Evaluation Days Left:       15
   Remote Agent Module Evaluation Days Left:     15
   Remote Agent Module Licenses:             0 Occupied / 1 Total
   Secure Forms Module Evaluation Days Left:     15
   SFTP Module Evaluation Days Left:         15
   Timer Event Module Evaluation Days Left:      15
   Workspaces Module Evaluation Days Left:       15
   Workspaces Module Licenses:               0 Occupied / 100 Total
```

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

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

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

Windows Account for the EFT 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 service to the account, and log EFT on as a service. Security policies should allow user accounts to log in locally.

The EFT 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 service, and you will need to reset permissions on the computer on which the EFT 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

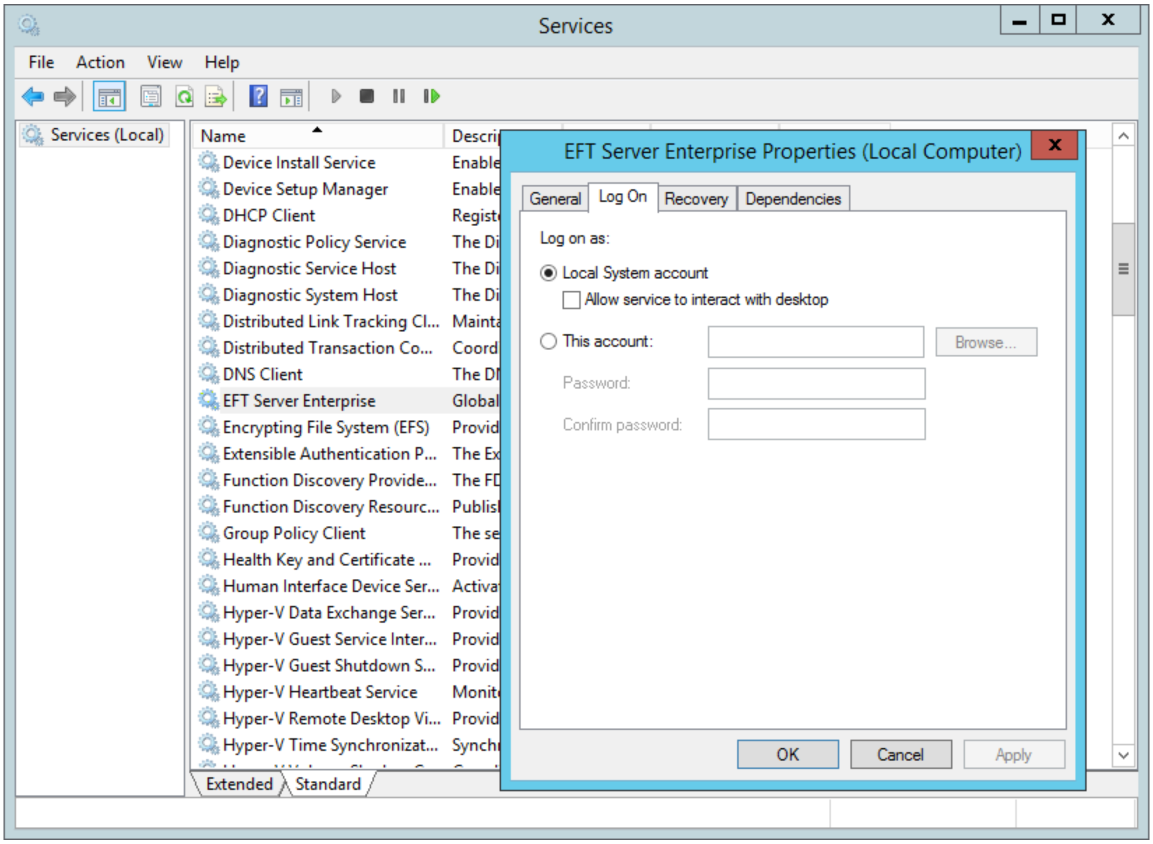
1. In Windows File Explorer, right-click the file or folder, then click **Properties**.
2. On the **Security** tab, click **Permissions**. The appearance of this dialog box is slightly different for files and directories and for different versions of Windows (W2K, XP, etc.).

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**.



Name	Descri
Device Install Service	Enable
Device Setup Manager	Enable
DHCP Client	Regist
Diagnostic Policy Service	The Di
Diagnostic Service Host	The Di
Diagnostic System Host	The Di
Distributed Link Tracking Cl...	Mainta
Distributed Transaction Co...	Coord
DNS Client	The DI
EFT Server Enterprise	Global
Encrypting File System (EFS)	Provid
Extensible Authentication P...	The Ex
Function Discovery Provide...	The FD
Function Discovery Resourc...	Publis
Group Policy Client	The se
Health Key and Certificate ...	Provid
Human Interface Device Ser...	Activa
Hyper-V Data Exchange Ser...	Provid
Hyper-V Guest Service Inter...	Provid
Hyper-V Guest Shutdown S...	Provid
Hyper-V Heartbeat Service	Monit
Hyper-V Remote Desktop Vi...	Provid
Hyper-V Time Synchronizat...	Synch

Log on as:

● Local System account

□ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

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

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? for details.

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

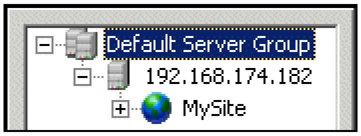
1. Close all unnecessary applications so that the installer can update system files without rebooting the computer.
2. Start the installer, and then click **Next**.
3. After installation components are loaded, the **Welcome** page appears.
4. Read the **Welcome** page, and then click **Next**. The **License 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.

10. Click **Finish**. The administration interface appears and the **EFT Server administrator Login** wizard appears.
11. 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.
12. Click **Next**. The **EFT Administrator Login** page appears.
13. 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.

14. 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 Migration wizard 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 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 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 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 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.

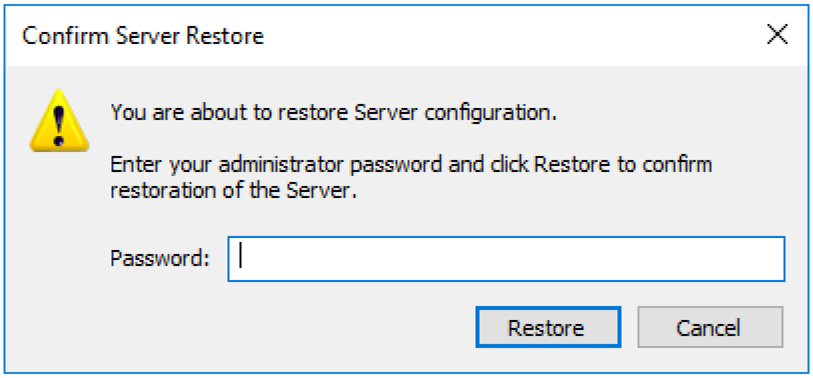
Backups from IPv4-only EFT versions will listen only on IPv4 addresses; if all listeners selected for administrative connections are unavailable, then switch to listening on localhost.

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.



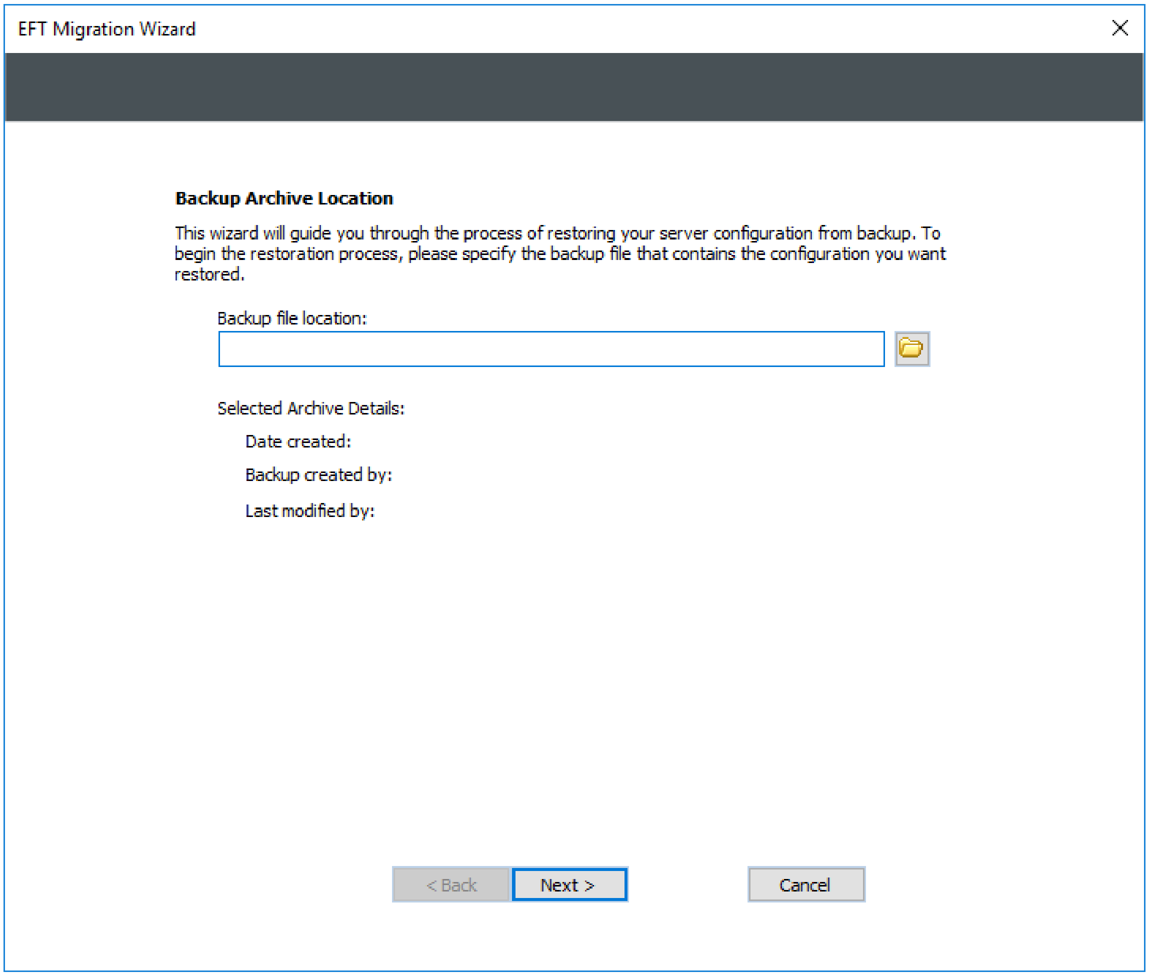
Confirm Server Restore

You are about to restore Server configuration.

Enter your administrator password and click Restore to confirm restoration of the Server.

Password:

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.



EFT Migration Wizard

Backup Archive Location

This wizard will guide you through the process of restoring your server configuration from backup. To begin the restoration process, please specify the backup file that contains the configuration you want restored.

Backup file location:

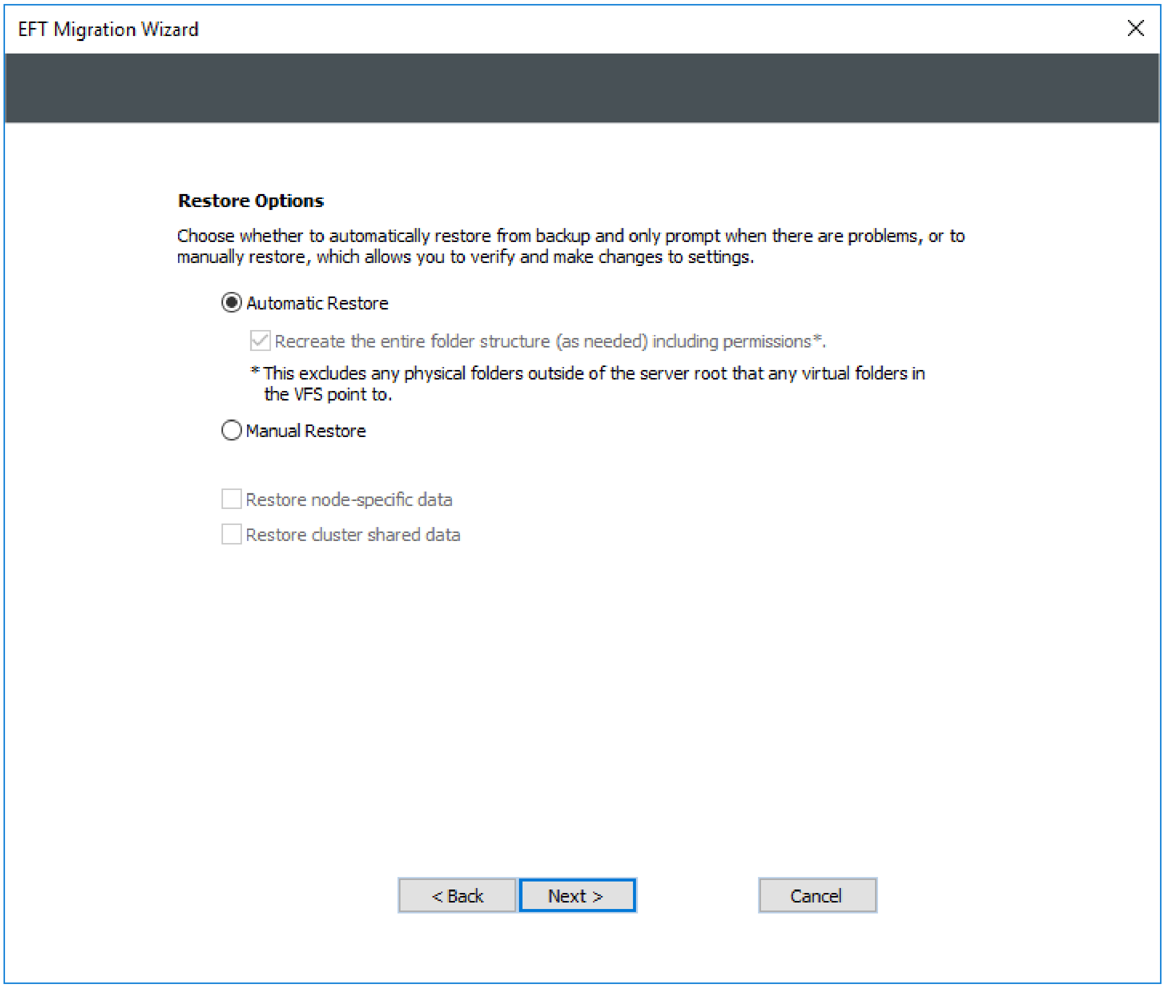
Selected Archive Details:

Date created:

Backup created by:

Last modified by:

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.



Restore Options

Choose whether to automatically restore from backup and only prompt when there are problems, or to manually restore, which allows you to verify and make changes to settings.

● Automatic Restore

☑ Recreate the entire folder structure (as needed) including permissions*.

* This excludes any physical folders outside of the server root that any virtual folders in the VFS point to.

○ Manual Restore

□ Restore node-specific data

□ Restore cluster shared data

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

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

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

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

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

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

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

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

   The **Server Administration Connectivity** page appears.
b. Review the IP address for each Site. If you are restoring a Site to a different IP address, click to edit the IP address in the **New IP Address Assignment** list. The **Sites to Restore** page appears.
c. Click **Next.** Select the check boxes of the Sites whose settings you want to import and clear the check boxes of the Sites whose settings you do not want to import.
d. Click **Next**. In the **Site Listening IP Address Assignment** page appears. Click the links to specify one or more IP addresses to use (or All Incoming), and then click **OK**.
e. Click **Next**. The **Site Authentication Manager Settings** page appears.
f. The authentication database for each Site to be restored appears in the list. In the **Settings** column, click **View/Modify** if you want to view or change the path where EFT will store the user database. (You cannot change the type of authentication.)
   - If EFT cannot connect to the Site's authentication provider, an error message appears.
   - Click **OK** to continue as is or click **Cancel** to modify the authentication provider settings.
g. Click **Next**. The **Site Root Folder** page appears.
h. Review the root folder location for each Site that you are restoring. If necessary, click the folder icon to specify a different location, and then click **Next**.
i. If the DMZ Gateway is defined and configured in EFT that you are restoring, the **DMZ Gateway** page appears. If not, skip this step.
   i. Review the IP addresses and ports for the DMZ Gateway. Click to edit the IP address or port, if different.
   ii. Click **Next**. EFT will test the DMZ Gateway connection and, if successful, the wizard proceeds to the next page.
   - If a failure occurs, the wizard displays a warning prompt indicating failure to connect to the DMZ Gateway and allowing you to either fix the problem (go back to the previous page to verify the IP address and port) or proceed

anyway (if the IP address and port are correct, but the DMZ is not communicating).

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

k. Click **Next**. Database connectivity is again verified and the **Ready to Restore** page appears.

l. Read the information on the page, and then click **Restore**.

m. A message appears indicating whether the configuration was successfully restored. Click **OK**.

n. Review the log if errors were encountered during restore.