

Upgrading EFT Server v5.x - v6.5.x

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v5.x through v6.5.x
- Refer to <https://kb.globalscape.com/KnowledgebaseArticle11194.aspx> for details of upgrading EFT v7 and later
- If you are upgrading from Secure FTP Server, refer to: [Upgrading Secure FTP Server v3.3 to EFT Server v6.x](#)

EFT can only be upgraded from up to two versions prior to the current version. Upgrading is supported from:

EFT SMB:

- EFT v5.x to EFT Enterprise v6.2.31 (EFT v5.x is not upgradable to EFT **SMB** v6.2.31)
- EFT SMB v6.2.3.1 or v6.3.x to EFT SMB v6.4.x (*If your current version is older than 6.2.31, you must upgrade to v6.2.31 first, then you can upgrade to version 6.4.x.*)
- EFT SMB v6.3.x or v6.4.x to EFT SMB v6.5.x
- EFT SMB v6.4.x or v6.5.x to EFT SMB v7.0.x
- EFT SMB v6.5.x or v7.0.x to EFT SMB v7.1.x

EFT Enterprise:

- EFT Enterprise v6.2.3.1 or v6.3.x to EFT Enterprise v6.4.x (*If your current version is older than 6.2.31, you must upgrade to v6.2.31 first, then you can upgrade to version 6.4.x.*)
- EFT Enterprise v6.3.x or v6.4.x to EFT Enterprise v6.5.x
- EFT Enterprise v6.4.x or v6.5.x to EFT Enterprise v7.0.x
- EFT Enterprise v6.5.x or v7.0.x to EFT Enterprise v7.1.x

You can upgrade from EFT SMB to EFT Enterprise **within the same version**; (*requires purchase of Enterprise license*):

- EFT SMB v6.2.31 or v6.3.x to EFT SMB 6.4.x (*If your current version is older than 6.2.31, you must upgrade to v6.2.31 first, then you can upgrade to version 6.4.x.*)
- EFT SMB v6.4 to EFT Enterprise v6.4
- EFT SMB v6.3 to EFT Enterprise v6.3
- EFT SMB v6.4 to EFT Enterprise v6.4
- EFT SMB v6.5 to EFT Enterprise v6.5
- Secure FTP Server v3.x to EFT Server (SMB) or Enterprise v6.2.31 (*This is the only upgrade path available for Secure FTP Server v3.x. Refer to <https://kb.globalscape.com/KnowledgebaseArticle10667.aspx> for more upgrade information regarding Secure FTP Server.*)

*Notes:

- If your current version is older than 6.2.31, you must upgrade to v6.2.31 first, then you can upgrade to version 6.4.x.
- Secure FTP Server 3.3.10 and EFT Server 5.2.22 are upgradable to 6.2.31 (we have seen issues otherwise). Any versions of Secure FTP 3 and EFT Server 5 older than 3.3.10 or 5.2.22 must be upgraded to those interim versions first.

- EFT Server 5 and Secure FTP Server are no longer supported products, and are not compatible with Windows 2008.
- Go to the **Discontinued Programs** section on <http://www.globalscape.com/support/reg.aspx#older> for older version downloads.

Before upgrading, refer to the "Upgrading the Software" topic in the [Online Help](#) for the version that you are upgrading to for caveats specific to the new version.

For liability reasons, it is Globalscape policy to not perform the upgrade or migrate the servers of our clients. Globalscape Support is instructed to only provide instructions or guidance, such as this article, for upgrading or migrating the server. While Support does not upgrade or migrate servers for our clients, you can purchase an upgrade package (with a liability waiver) from our [Professional Services team](#) to have them personally handle the process or provide dedicated Non-Standard Support hours to have a qualified Server Support Analyst assist during a scheduled non-business period. Please contact Support or your Account Manager to receive a quote and schedule a time for the upgrade.

- **DMZ Gateway:**
 - If you are also upgrading DMZ Gateway, upgrade DMZ Gateway first, then upgrade EFT.
- **ARM:**
 - **In v6.5 and later**, a more sophisticated process is used to upgrade the ARM database. Refer to "Upgrading the EFT Database," "Upgrading Large Databases," and "ARM Database Schema Change Tracking" in the help documentation for your version of EFT for important information.
 - **When upgrading from versions prior to EFT v6.4**, if you upgrade the SQL Server ARM database with the installer, the default schema name is now dbo.
 - During updates or upgrades, EFT needs full DB Owner access to update the schema. Once it is set up, EFT Server only needs to be able to read, write, and execute stored procedures. Refer to the Knowledgebase article "[Configuring EFT Server Permissions in SQL Server](#)" for more information.
- **API:**
 - **In v6.5 and later**, COM API resources including SFTPCOMInterface.DLL and associated files are saved in C:\Program Files\Common Files\Globalscape\SFTPCOMInterface so that they can be shared with other Globalscape applications, such as Mail Express, ensuring that each application is using the same DLL.
 - **Any older scripts that use the v6.2 COM API** for Timer Events must be manually updated to the new API.
 - The [IP Access/IP Ban has increased functionality](#), and the COM interface has been modified to match the new functionality.
- **WTC:**
 - (Java-enabled version) When upgrading the WTC, workstations might receive a Java error, but then the WTC will load and be functional. Refer to [KB article#10654](#) for details.
 - When upgrading, the `\web\custom\` and `\web\public\` folders are backed up and renamed with the date and time (e.g., `\customBackup_9-28-2010_16-18\` and `\publicBackup_9-28-2010_16-18\`). The new versions of the files may have some updated content, so rather than overwriting the new files with your old files, you should manually copy your customizations to the new files after upgrading. This applies to any edits for the per-Site and per-Server login pages, Web Transfer Client (WTC) interface, Account Management interface, and AS2 Management interface.
 - End users will need to clear their browser cache: refer to KB <https://kb.globalscape.com/KnowledgebaseArticle10654.aspx> for more information.
 - FTP requires UPLOAD permission in addition to APPEND to resume a partial file transfer.
- **Event Rules:**
 - **In v6.4 and later**, the Folder Monitor Event Rule trigger provides better reliability for the handling of file events. The current Folder Monitor algorithm uses more resources (threads) than the v6.2 algorithm. An EFT with more than 250 Folder Monitor Rules should use the v6.2 algorithm, which uses fewer resources. **The 6.2 Folder Monitor algorithm** can be [selected via a registry key](#).
 - The Event Rule file Copy/Move wizard provides control for overwrite options. The overwrite options were set in earlier versions using registry keys. Any associated registry keys will now be ignored and you should update your Event Rule Actions with the desired overwrite option.
 - EFT supports PORT mode when using the SOCKS protocol to the outbound gateway/proxy. Event Rules that were configured for **SOCKS PORT mode in v6.2**, will switch from acting as a PASV mode connection to a PORT mode connection in later versions.
 - During the upgrade, if a non file-trigger rule contains an `%FS.FILE_NAME%` variable, it will be converted to `%SOURCE.FILE_NAME%` and a WARNING will record the change in the EFT.log. Refer to Variables (List) for more information about the `%SOURCE.FILE_NAME%` variable.

- By default, IP Access-related Event Rules are limited to 1000 rules. If you upgrade with more than 1000 denied IP addresses, the rule count overflows and you cannot create new rules. Refer to Knowledgebase article "[Cannot create new Event Rules after upgrading](#)" for a registry fix.
- **EFT v6.5** uses UTF-8 for RADIUS/RSA. **When upgrading to v6.5**, in cases where ASCII strings with >127 characters were used for RADIUS in the prior version, there is some risk of loss of fidelity when converting to UTF-8 (depending on the code page) for **v6.5 or later**. You may need to re-enter values, disable and then re-enable RADIUS, or restart the Site to refresh the values.
- If a Site uses the LDAP Authentication Manager, and if the users are allowed to change their passwords, LDAP calls are used to make the password changes. In v6.2, Active Directory calls were used to make the password changes. With the switch to LDAP **in v6.3 and later**, LDAP over SSL should be used to protect the password changes. LDAP over SSL can be difficult to configure, so the registry setting in <https://kb.globalscape.com/KnowledgebaseArticle10659.aspx> allows you to continue using the Active Directory API for the password changes, which also provides security for the communication path.
- If NTLM v2 proxy authentication support is needed, the default HTTP client must be changed from the Apache HTTP client to the Java JSE HTTP client. The JSE HTTP client does not properly set the Content-Length for files > 2GB, so a custom X-Header is used to communicate the file size. Any HTTP proxy that is in the path between the browser and EFT must properly pass the custom X-Header. Refer to [Accessing EFT Through a Proxy](#) for details.
- It is a good idea to read the [Release Notes](#) before you begin.

DISCUSSION

The process for upgrading EFT, whether Enterprise or SMB, is very straight forward and should take no more than 45 minutes, if everything is done properly. (If you want to move EFT to a different computer, you should read this [separate article](#) for that process FIRST.)

Prepare:

1. Ensure that the version of EFT to which you are upgrading is compatible with your server by viewing the system requirements for that version. Refer to <http://help.globalscape.com/help/> for the system requirements for your version.
2. Request and receive from your account representative a new EFT license, if necessary, and a new DMZ Gateway v3 license, if are using DMZ Gateway, and the installers.
3. Stop the EFT Server service to ensure all settings are preserved. (After the FTP.cfg copy is complete, later in this procedure, the service can be restarted.)
4. Create a backup of the EFT Server data directory:
 - Windows 2003: **C:\Documents and Settings\All Users\Application Data\GlobalSCAPE\EFT Server**
 - Windows 2008: **C:\ProgramData\GlobalSCAPE\EFT Server**
5. Export a copy (backup) of the registry.
6. If the Auditing and Reporting Module (ARM) is active, create a backup of the EFT database.

Upgrade:

1. Use the installer to upgrade EFT and, if you use ARM, update the database. (Instructions are available in the [online help](#).) Before clicking **Finish**, clear the check box used to start the service. (That is, do NOT start the service yet.)
2. Add the EFT server service account in Windows to run the EFT server service (if there isn't one from your previous version). Ensure that the EFT server service account has full rights to the application data directory and the site data directory.
3. Start the EFT server service.
4. If upgrading from a version prior to EFT v6, register EFT (all modules will have remained registered).
5. If you use or will be using the Secure Ad Hoc Transfer module or DMZ Gateway module, use the corresponding installers to install or upgrade.
6. If you will be using the DMZ Gateway module, in the EFT administration console, activate the DMZ Gateway 3 serial number. (Click **Help > Activate DMZ Gateway Module**).
7. Verify that the EFT Sites are working properly by testing connections, Event Rules, and reports.

Rollback:

1. Uninstall the newer EFT version.
2. If nothing else changed between the EFT install and rollback process, restore the registry.
3. Install the previous EFT version, skipping the ARM portion; before clicking **Finish**, clear the check box to start the service.
4. With the EFT service stopped, paste the backup of the previous EFT version folder over the default location:
 - Windows 2003: **C:\Documents and Settings\All Users\Application Data\GlobalSCAPE\EFT Server**
 - Windows 2008: **C:\ProgramData\GlobalSCAPE\EFT Server**
5. Start the EFT Service.
6. If the Auditing and Reporting Module (ARM) was active, restore the ARM Database (be aware that the reports will not function until the restore is complete).
7. Verify that the EFT sites are working properly by testing connections, event rules, and reports.

The following links provide reference information concerning the upgrade or migration process:

- Upgrading EFT: <http://help.globalscape.com/help/eft6-4/UpgradingSoftware.htm> (or your version of the help in <http://help.globalscape.com/help/>)
- Migrating EFT: <https://kb.globalscape.com/KnowledgebaseArticle10251.aspx>

If you need help upgrading, the Technical Support Team can be reached at 210-366-3993 or via the [Online Form](#) during our regular office hours Monday through Friday, from 8:00 AM to 6:00 PM CDT (GMT -5). Our offices are closed on weekends and for major US holidays.

Posted 6 Years Ago by [GlobalSCAPE 5](#)
<https://kb.globalscape.com/KnowledgebaseArticle10665.aspx>