Enhanced File Transfer Server 4

User's Guide

globalSCAPE®

Table Of Contents

1

Enhanced File Transfer Server

GlobalSCAPE's Enhanced File Transfer Server (EFT) is a hardened file/data transfer server that provides secure data transactions over standard Internet protocols. Used together with DMZ Gateway and the EFT Web Transfer Client, Enhanced File Transfer Server provides a highly secure and reliable file management system. EFT Server highlights include:

- Multi-protocol support: (FTP, FTP (SSL/TLS), SFTP (SSH2), HTTP/S)
- Post-transaction processing using highly configurable event rules
- Data reliability and integrity guarantees
- Repository encryption based on OpenPGP standards
- Automation of complex and time-consuming tasks
- Local and remote administration of multiple servers and/or sites
- Flexible authentication choices
- Highly configurable user, account, and site settings

Data Protection and Encryption

EFT Server protects intellectual property, trade secrets, and customer files transferred over the Internet using secure protocols including FTPS (SSL/TLS), SFTP (SSH2) and HTTP/S.

EFT Server helps meet regulatory and privacy requirements such as HIPAA, GLBA, and SB1386, by including OpenPGP technology for encrypting, decrypting, and signing files stored on disk. EFT Server also includes provisions for off-loading files to another server securely or to a network share.

DMZ Gateway

This optional server is designed to reside in the demilitarized zone and provide secured communications with EFT Server behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ.

EFT Web Transfer Client

This optional client is a browser based file transfer client that allows users to upload and download files to an EFT server using a connected web browser. It gives your users a transparent way to connect, and you don't have to install anything on the client end—the client deploys automatically from EFT Server if you have a license.

Tracking and Auditing

Secure data delivery requires strong audit trails for tracking and non-repudiation. EFT Server provides industry standard logging (W3C, NCSA, Microsoft IIS Extended), E-mail notification of completed transactions, and digital certificates for proof of identity.

Standards Compliance

EFT Server enables secure, reliable file transfers using standard FTP or HTTP clients, including Web browsers or secure FTP clients such as CuteFTP Professional.

Guaranteed Delivery and Data Integrity

EFT Server extends the industry standard FTP and HTTP protocols with enterprise-class reliability features, including post transmission integrity verification, mid-file recovery, and automatic restart.

Programmatic Interface

EFT Server can be controlled through its Windows Administrator Interface, or through its Component Object Model (COM) interface. The COM API is a programmatic interface that lets you control the server from your own custom applications using any COM enabled programming language.

Accelerated Transfers

EFT Server supports Multi-part (segmented) transfers for faster delivery of large files over large geographical distances. Multi-part transfers require the use of compatible clients such as CuteFTP Professional.

Life-Cycle Management

GlobalSCAPE EFT Server lets you quickly and efficiently manage the removal of users, manage temporary accounts, address the revocation and if necessary re-issuance of expired or compromised public-keys or certificates.

Authentication and Authorization

EFT Server supports password, public-key, or one-time-password authentication. User profiles can be managed internally or externally through NTLM, Active Directory (AD) or ODBC data sources.

User and Group Management

Manage system resources including bandwidth, folder access, file types and more using granular or site-wide controls provided for user and group management. Visually manage folder permissions via Explorer-like Virtual File System view. Inherit or override permissions, grant administrative, guest, or anonymous permissions or deny access altogether.

Support

Questions? Navigate to http://www.globalscape.com/support for information on customer service, technical support, software registration, product manuals, and downloads, as well as access to GlobalSCAPE's Knowledge Base and FAQs.

What's New in EFT 4

DMZ Gateway

Secure data transmission through a demilitarized zone (DMZ). A DMZ Gateway in the DMZ handles all EFT Server requests and keeps all data safely behind the firewall. No outbound holes in the firewall, no data is ever stored in the DMZ, and no user database replication is needed.

Streaming Repository Encryption

Encrypt files stored on disk in the Virtual File System as they are read from or written to disk. Streaming repository encryption ensures that only encrypted data is ever stored on disk.

Streaming Compression

Accelerate transfers for clients supporting the new MODE Z command through compression of transfers on-the-fly.

Connection Monitoring

Troubleshoot problem connections with connection monitoring. Examine per-connection logs in real-time, search for text, filter results, and configure monitoring options.

Status Monitoring

View information and statistics on the selected connection, including the last three files downloaded, current directory, originating IP, and more.

Event Rules enhancements

Refine post processing automation even further with EFT's enhanced event rules logic. Monitor local folders for changes, change the order rule actions occur, retrieve remote files, specify failure actions, specify actions when data is added or changed in specified folders, or use wildcards to specify conditions.

2

Install and Register

Install

To install Enhanced File Transfer Server

1. Start the installation wizard and follow the instructions.
2. Select the components you want to install. You can:
    - Install **EFT Server** (cftpte.exe) and **EFT Administrator** (cftpsai.exe) together.
    - Install only **EFT Administrator** for remote administration of **EFT Server**.
3. Create a user name and password for the Administrator account for connecting to EFT Server from the EFT Administrator. Remember your user name and password; you need them to connect to EFT Server.

Register

You must register Enhanced File Transfer Server with either a serial number or a trial serial number before you can use it.

Register Online (You must be connected to the Internet)

1. Start the EFT Administrator
2. Enter your user name and password to connect to the EFT Server.
3. If you are registering a trial use, select **Enter Trial Serial Number**.
4. If you are registering a purchased license, select **Enter Serial Number**.

> **Note:**
> If you are registering a purchased serial number, you can also select **Enter EFT Serial Number...** from the Help menu.

5. Enter your serial number in the Serial Number field.
6. In the name field, enter your name and/or your company name.
7. If you are behind a proxy, select **Proxy** and configure the proxy settings accordingly.

Note:
If a firewall or a proxy server is in use, your network administrator should ensure that port 80 is open during the registration process.

8. Select **Register**.
9. You should receive a message confirming registration. Click OK.

Note:
Registration must be performed through the EFT Administrator on the server computer. You cannot register through a remote installation of the EFT Administrator.

Register Manually (You should have access to a computer that connected to the Internet, or access to an email account.)

If you have problems with the registration process, or if the computer you are installing EFT Server on does not have Internet access, try registering the software manually.

1. Follow Steps 1-7 from Register Online
2. Check the **Register manually** checkbox.
3. Provide the necessary information in the fields that appear.
4. Select **Register**.
5. The Manual Registration dialog appears. Select **Copy to Clipboard**.
6. If the computer you are installing the software on has Internet access and a compatible browser, select **Register on the web**. A browser window appears pointed to the GlobalSCAPE Manual Registration web page. Follow the instructions there.
7. If registration is successful, a .reg file download prompt appears on your browser. Save the file, and transfer it to the desktop of the computer you are installing the software on.
8. Make sure that the Windows System Service (GlobalSCAPE EFT Server) is stopped before you write the .reg file to your registry. See Configuring the server as a Windows service for more information.
9. Double-click on the saved file in order to write the information to your registry.
10. Once the registry is successfully updated you can safely delete this file.
11. Restart the Windows System Service (GlobalSCAPE EFT Server). See Configuring the server as a Windows service for more information.
12. Cancel or close any open registration dialog boxes in EFT Administrator, then exit the Administrator and restart it.

Note:
You can also email the manual registration information to GlobalSCAPE Technical Support. GlobalSCAPE will confirm your registration and send you the .reg file. You can send the email from any computer with

Internet access; just remember to transfer the .reg file back to the computer you are installing the software on.

3

Setting Windows System Services

Starting and stopping EFT Server

Enhanced File Transfer Server starts automatically and runs as a Windows system service. If you close EFT Administrator, the Enhanced File Transfer Server continues to run in the background as a system service.

To start or stop the EFT Server with the EFT Administrator

1. In EFT Administrator, select **Service Applet Settings...** from the Edit Menu. The **Transfer Engine Service Settings** dialog appears.
2. Select **Start service** (or **Stop service**) and close the **Transfer Engine Service Settings** dialog box.

To start or stop the server using the Services option in the Control Panel

1. In Windows XP or 2000, select **Start**> **Settings**>**Control Panel**>**Administrative Tools**>**Services**.
2. Select **GlobalSCAPE EFT Server** from the Services list.
3. Right-click or double-click and select **Start** (or **Stop**).
4. Close the Services and Administrative Tools windows.

To start or stop the server from the command line

1. Select **Start** > **Run**.
2. Enter **cmd** or **command**.
3. Select **OK**.

4. To start the EFT Server, enter **Net start "globalscape eft server"** at the prompt. (include the quote marks).
5. To stop the EFT Server, enter **Net stop "globalscape eft server"** at the prompt. (include the quote marks).
6. After the service is started or stopped enter **Exit**.

Note:
If **Install service** is the only button enabled in the Transfer Engine Service Settings window, select it, then select **Start service**.

WARNING:
Any time you run a server, you expose your computer to outside users. There is the potential for exposing files and programs on your computer and network to malicious outside users, particularly should the server become compromised.
Although you can set folder permissions from within the Server Administrator, you can add an extra level of protection by establishing a user account for the server and then limiting folder access through the server's user account permissions. This establishes a stopgap until server/system integrity can be restored should the server ever become compromised.

To configure the server to run securely, you should:

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

Starting and stopping EFT server remotely

To start or stop the EFT Server remotely

1. In EFT Administrator, select **Service Applet Settings** from the Edit Menu. The **Transfer Engine Service Settings** dialog appears.
2. Under Connection, select **Administer remote machine**. Enter the IP address of the server you want to administer.
3. Select **Connect to Service Manager**.

Note:
The remote EFT Administrator you are logged on to passes your user name and password to the Windows System Services on the computer running the EFT Server. The account you log on with must have administrative rights on that server to make any changes to the GlobalSCAPE EFT Server service running on it.

4. Select **Start service** (or **Stop service**) and close the Transfer Engine Service Settings dialog box.

Creating a user account for the server

In order to run **Enhanced File Transfer Server** securely as a service, you need to create a user account for it in Windows.

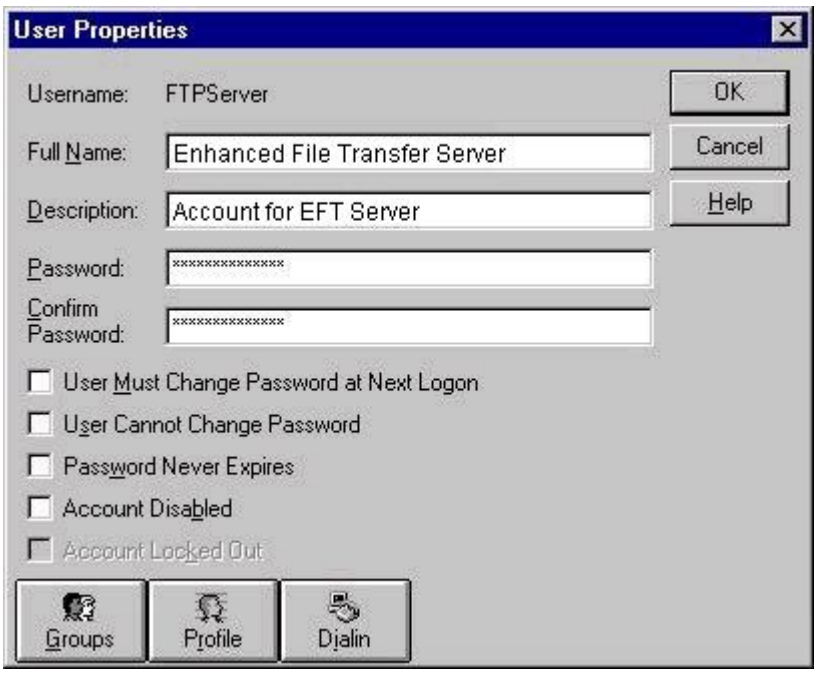
Note:
Setting up a user account increases security, but is not required to run Enhanced File Transfer Server.

To create a user account in Windows XP Professional or Windows 2000

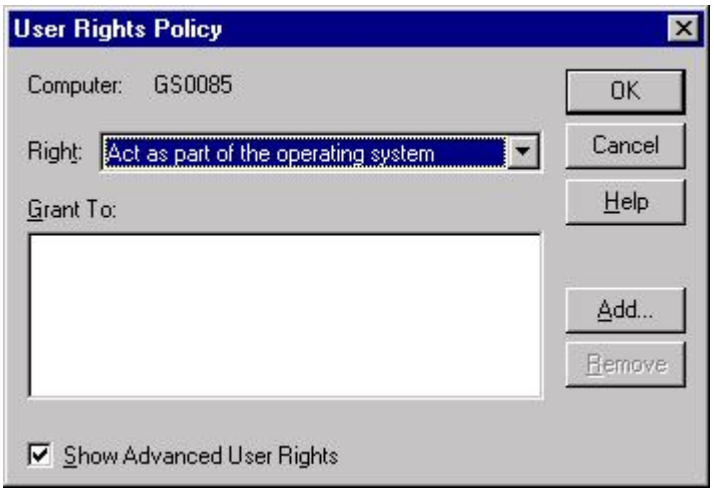
1. After you install the server, navigate to **Start > Settings > Control Panel> Administrative Tools > Computer Management**.
2. Select **Local users and groups > Users**.
3. Select **Action> New User** to launch the New User dialog
4. Enter the appropriate information in the New User dialog for an EFTServer user account.
5. Select **Create**.
6. Close the New User dialog box.
7. Close the Computer Management console.
8. From Administrative Tools, open **Local Security Policy**. If the Administrative Tools window is no longer open, navigate to **Start > Settings > Control Panel> Administrative Tools> Local Security Policy**.
9. Navigate to **Security settings > Local Policies > User Rights Assignment**
10. Double-click **Act as part of the operating system** under the **policy** column in the right-hand pane.
11. The **Local Security Policy Setting** dialog appears. Select **Add...**
12. The **Select Users or Groups** dialog appears. Select the new user you just added (**EFTServer**)**,** select **Add...** , then select **OK** twice to apply the change.
13. If necessary, Assign permissions for this user account in Windows.
14. Assign the server to the new user account and log the server on as a service.

To create a user account in Windows NT

1. After you install the server, navigate to **Control Panel > Administrative Tools > User Manager**
2. From the menu, select **File > New User** to create a new user account for **"FTPServer"**.
3. Enter appropriate information in all of the fields in the **User Properties** dialog box, as shown below.



4. Click **OK**.
5. From the menu bar, select **Policies > User Rights**. The **User Rights Policy** dialog will appear.
6. Enable the **Show Advanced User Rights** check box at the bottom of the dialog.
7. Select **Act as part of the operating system** from the drop-down box.



8. Click **Add**. The **Add Users and Groups** dialog will appear.

9. Make sure that the drop-down list at the top of this dialog has your own computer selected. Click the **Show Users** button and select **FTPServer** from the list
10. Click **Add**.
11. Click **OK** in both dialogs.
12. Assign permissions for this user account in Windows.
13. After assigning permissions, you should assign the server to the new user account you have created and then log the server on as a service.

Logging on the server as a service

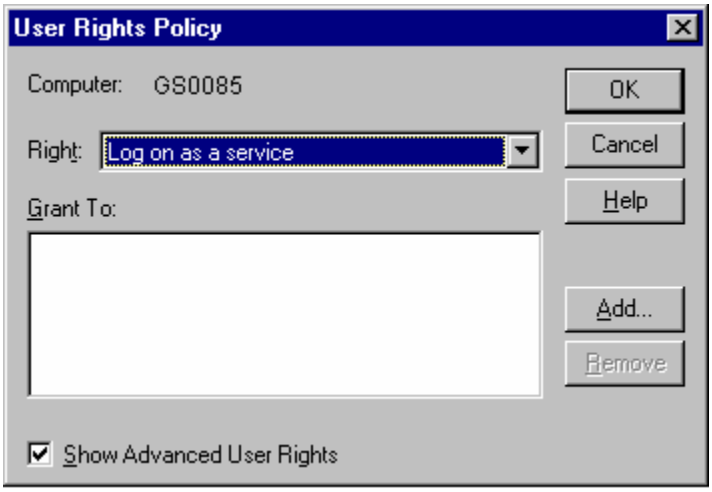
Note:
The logon as a service right is automatically granted in Windows XP Professional, 2003, and 2000.

Windows XP Professional, Windows 2003, and Windows 2000

1. Go to **Start > Settings > Control Panel> Administrative Tools > Local Security Policy**
2. Navigate to **Security settings > Local Policies > User Rights Assignment**
3. Double-click on **"logon as a service"** under the **policy** column on the right side of the window
4. Select **Add User or Group...** Select the user you want to add (**EFTServer**), select **Add...** , then select **OK** twice to apply the change.

Windows NT

1. Go to **Administrative Tools > User Manager** in your Windows NT operating system.
2. From the menu bar, select **Policies > User Rights**. The **User Rights Policy** dialog will appear.
3. Select the **Show Advanced User Rights** check box at the bottom of the dialog.
4. Select **Log on as a service** from the drop-down box.



5. Click **Add**. The **Add Users and Groups** dialog will appear.
6. Make sure that the drop-down list at the top of this dialog has your own computer selected. Click **Show Users** and select **EFTServer** from the list
7. Click **Add**.
8. Click **OK** in both dialogs.

Assigning permissions for EFT Server user account in Windows NT

Using Window's permissions, set the permissions for folders, files or drives for this new user account to be as restrictive as possible while still allowing the server enough permissions to run. After carefully determining what files and folders your users will need to access, gradually increase the permissions.

Windows NT permissions can be edited through the **Security** tab in the **Properties** of an object (such as a folder or file object in Windows Explorer). On the **Security** tab, select the **Permissions** button to display and edit the permissions for the object. The appearance of this window is slightly different for files and directories and for different versions of NT (W2K, XP, etc.).

Keep in mind that you have the option to grant or withhold read and write permissions. Read-only permissions are the most secure. 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 or HTTP Servers will not need ***any*** access to these directories at all.

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

Please refer to the Windows Help documentation for your specific operating system for more information on setting permissions to folders and files.

Windows NT permission rules

In order to secure your system, GlobalSCAPE recommends that you create an user account for the server and grant restrictive permissions to that user account. When you are assigning permissions to individual folders or directories in Windows NT, you may want to reference the following three rules. These rules differ somewhat from the VFS rules that govern **EFT Server** permissions.

Three rules determine the permissions that are ultimately granted to a user in Windows NT:

1. **Explicit denial: All users or groups assigned "No Access" have no access**

   If the user, or a group that the user is in, has been assigned "No Access", that user is explicitly prohibited from using the file, folder or drive. No other permissions will change this.

2. **Cumulative permissions: Permissions are combined when a user is not explicitly denied access**

   If the user is not explicitly denied access, the user's permissions will be combined. For example, if user Cal is given read and write permissions for Folder1, and Cal is also in a group that is given execute permissions for that folder, then Cal will be able to read, write and execute files in Folder1.

3. **Implicit denial: A user or group that has never been granted any access at all will not be given access**

   If the user, or a group containing the user, is not granted any permissions, that user or group will be denied access. Access must be specifically granted.

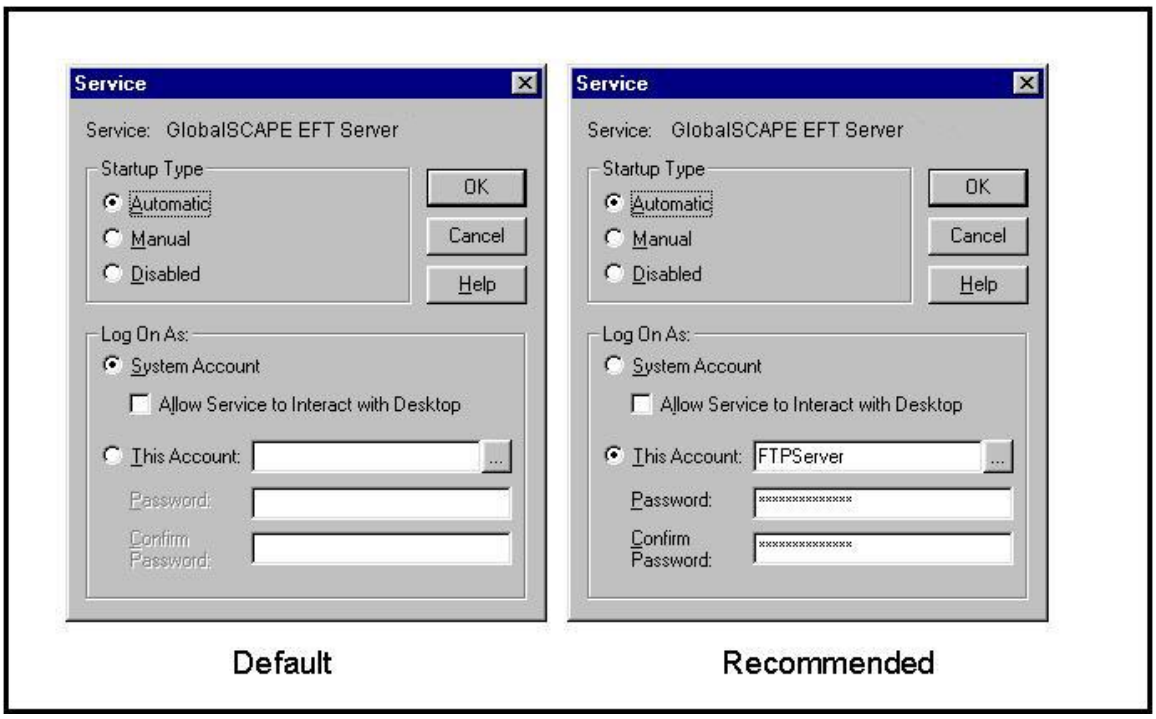
Assigning the service to a NT user account

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

To assign the service to an NT account

1. Click on the Windows **Start** button, select **Settings > Control Panel > Services**. *(W2K Control Panel > Administrative Tools > Services.)*
2. Select **EFTServer** from the list of services and double-click or press the **Startup** button. The **Service** dialog box, depicted below for Windows NT, will appear.
3. Below **Log On As**, change the service from a **System Account** to **This Account**.
4. Select the **EFTServer** user account you created previously.

5. Click **OK**.
6. You will need to restart the system in order for the change to take effect.

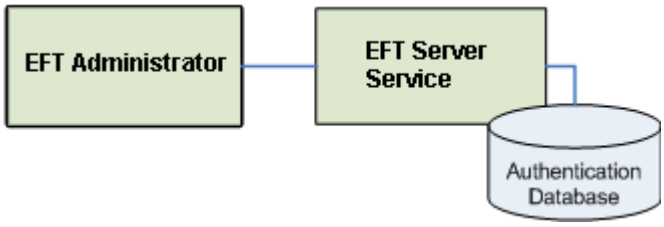


4

Using the EFT Administrator

The EFT Administrator

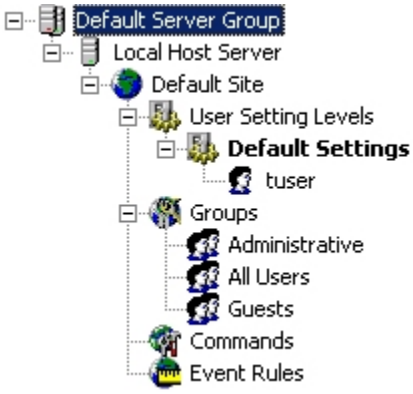
Enhanced File Transfer Server is configured and maintained through the EFT Administrator. Creating Server Groups, Servers, and Sites, managing user accounts and permissions, setting security protocols, setting up commands, configuring event rules: everything you do with EFT Server can be managed through the EFT Administrator. The EFT Administrator connects to the server on either a local or remote computer. You can install the EFT Administrator on as many computers as you like, but the EFT Server may only be installed on computers with valid Enhanced File Transfer Server software licenses.



The EFT Administrator opens when you select EFT Server from the start menu or desktop. By default, the EFT Server itself runs when the Windows OS boots up on the server. You must connect to an EFT Server to make any changes to it.

EFT Inheritance

Enhanced File Transfer Server employs an inheritance hierarchy to manage its server, site and user settings, and group permissions. The EFT Administrator displays this hierarchy as a navigation tree in the left-hand pane (Server tab).



Server Groups are the topmost level. It contains Servers, Sites, and everything else beneath it. This is an organizational function for multiple groups of Servers and you can add an additional Server Group.

Servers represent one or more physical file transfer server (Server Engine) running on your local or remote system.

Multiple **Sites** (or hosts) are allowed within each Server. Sites are like virtual FTP servers bound to one or more IP address. Configuration of site-wide settings can be inherited at lower levels (at the User Setting Level or User levels).

User Setting Levels allow you to apply a setting configuration to an entire group of users. Setting Levels are a powerful way of organizing users into groupings with pre-defined settings. One Setting Level may by quite restrictive, while another may be quite liberal. Power users would be assigned to a level allowing greater flexibility in using server resources while guest users would be assigned to a more restrictive level, limiting access and use of server resources.

Users are individual clients assigned a Setting Level. Each user can be configured to inherit settings from the User Settings Level or have specific settings defined for that particular user.

Permission **Groups** allow the administrator to define access permissions to files and folders. Groups are assigned at the Site level. Users assigned to a Group have their access to folders and files defined by Group permissions. Group permissions are covered in more detail elsewhere in this document.

Commands and Event Rules - see Chapter 10, Automation.

Connecting to a server

To connect to a *local* server

1. Launch EFT Administrator.
2. Select the server you want to administer. (You can manage multiple EFT Servers with a single EFT Administrator.)
3. On the menu bar, choose **File > Connect to EFT Server.** The **Connect to EFT Server** dialog box appears.
4. Enter your administrator **Username**.*****
5. Enter your **Password**.*****
6. Select **Local Host**.
7. Select **Connect**.

*The administrator username and password is created during installation.

> **Note:**
> If there is an error when trying to connect to EFT Server, make sure that the Windows System Service for it is running.

To connect to a *remote* server

> **Note:**
> Before you can connect to a remote server, make sure you have the server configured for remote administration.

1. Launch EFT Administrator.
2. In the left pane, select the server you want to connect to.
3. On the menu bar, choose **File > Connect to EFT Server.** The **Connect to EFT Server** dialog box appears.
4. Enter your administrator **Username** if it wasn't entered automatically.
5. Enter your **Password**.
6. Select **Remote Host**.
7. In **Host**, enter the IP address for the remote server.
8. In **Port**, enter the Port number for the remote server.
9. Select **Connect**.

5

Server Groups and Servers

Server Groups and Servers

Server Groups

Server groups are at the top of Enhanced File Transfer's setting hierarchy and allow you to group multiple servers. You can add as many Server Groups as you need.

Servers

Servers control the settings for one or more EFT Servers, either locally or remotely. Servers consist of one or more physical file transfer server (EFT Server) running on your local or remote system.

Create, delete, and rename Server Groups

To create a new Server Group

1. In EFT Administrator, choose **File > Add New Group of Servers**. The **Create New Group** window appears.
2. In the **Group Name** box, type any name you want for the Server Group.
3. Select **OK**.

To rename a Server Group

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. In the left pane select the Server Group you want to rename.
3. On the menu bar, choose **Configuration > Rename**.
4. Next to the Server Group's icon, type any name you want for the Group.
5. Select **Enter** on your keyboard.

To delete a Server Group

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Server Group you want to delete.

3. On the menu bar, choose **File > Remove Group of Servers**.

Create a server

To create a new server

1. In the EFT Administrator, select **File > Add New EFT Server**. The **Add New Server** window appears.
2. In the **Name** box, type any name you want for the Server.
3. If the Server is on the same machine where you have opened the Administrator Interface, choose the **Local host** option and skip to step six. If the Server is on a different machine, choose the **Remote host** option and continue with step five.
4. In the **Host** box, type the IP address of the machine where the new server will be located.
5. In the **Port** box, leave the port at **1100** unless you want to use a different port to administer the server.
6. Select **Save**.

To delete a server

1. In the EFT Administrator, select the Server you want to remove. You should be connected to the server.
2. On the menu bar, choose **File > Remove Server**. A warning window appears, reminding you that your log in information will be lost.
3. Select **Yes**.

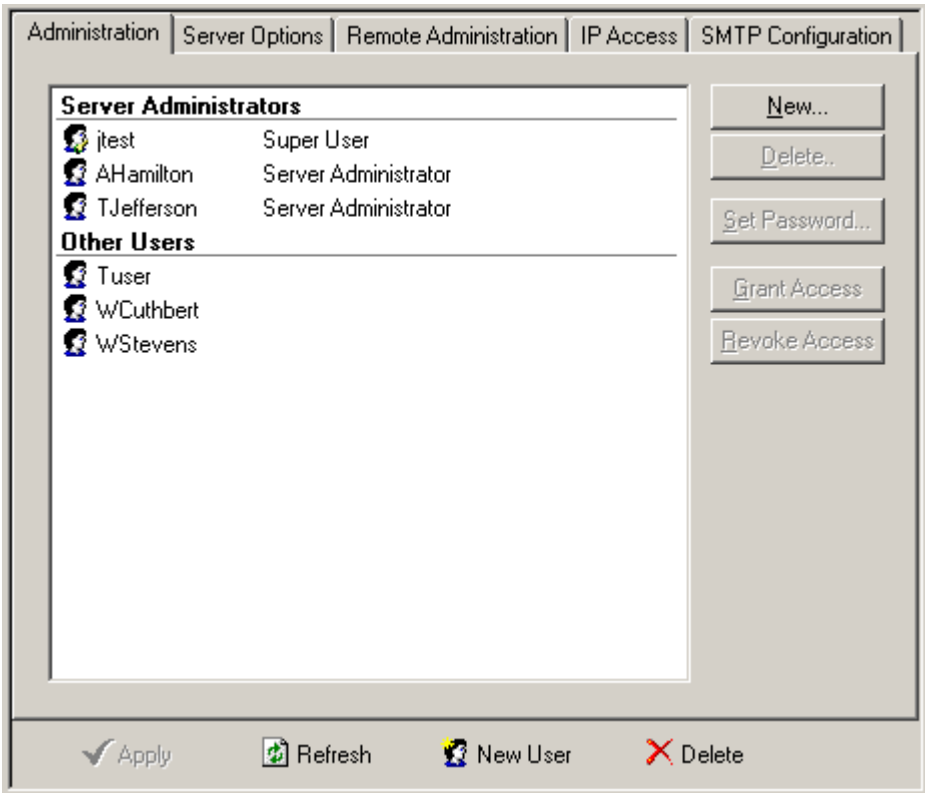
WARNING:
When you delete a Server, you also delete all of your login information—you must manually recreate it.

Adding server administrators

You can give other people access to the administrative functions of Enhanced File Transfer Server by creating an administration account for them in the EFT Administrator.

To create an server administration account

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Server you want to add an administrative account to from the left-hand navigation tree.
3. In the right pane, select the **Administration** tab.



4. Select **New...** and add a user name and password for the new administrator account.

Note:
Passwords are case-sensitive.

5. If you want the new account to have server administration rights, select **Allow server administration**. This gives the new account administration access to all sites associated with the selected server.
6. Select **OK**. The new account appears in the Administration list.
7. You can grant (or revoke) access to any user (except the Super User) by selecting the user and select **Grant Access** (or **Revoke Access**).

Note:
You can also select and drag a user from one list to another.

Note:
To set or create Site administrative accounts, see Adding Site administrators.

Updating the user information from the authentication database

You can set Enhanced File Transfer Server to automatically check the user authentication database at regular intervals to make sure the server's user information is correct and up-to-

date. This feature updates EFT Server only. You must manually refresh user information in the EFT Administrator in order to see changes on-screen.

To automatically update Transfer Engine authentication information

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Server you want to configure from the left-hand navigation tree.
3. In the right pane, click the **Server Options** tab.
4. In the **Default User Database Refresh Interval** list, select how often you want the Server Engine service to check for changes to the authentication database. If you do not want the service to check, select **Never refresh user list automatically**.

Note:
When you select **Refresh** in EFT Administrator it only checks the EFT Server service for updated user information. It does not check the authentication database.

Server log configuration

To monitor server activity, you can reference the server's log files. EFT Server supports W3C, Microsoft IIS and NCSA log file formats. Server events are logged to a file named [log file format]yymmdd.log. The log file format abbreviations used in the log file name are:

Log File Format	Abbreviation
W3C	Ex
Microsoft IIS	In
NCSA	Nc

To select a log file format

1. In EFT Administrator select the **Server** tab. You should be connected to the server.
2. Select the **Server Options** tab.
3. From the **Log file format** list, choose **W3C**, or **Microsoft IIS** or **NCSA**.

Note:
Changing the log file format disconnects all active users. It is recommended to stop all Sites or wait until all users are inactive before changing the log file format.

4. Select **Apply**.

Note:
The W3C format records all times in GMT (Greenwich Mean Time).

To select the log file output folder

1. In EFT Administrator select the **Server** tab. You should be connected to the server.
2. Select the **Server Options** tab.
3. In the **Folder to save log files** box, type the path for your server's log files. To browse for a path, select the yellow folder button.
4. Select **Apply**.

Note:
By default, log files are saved in the Enhanced File Transfer Server program folder.

To choose how often the log file is rotated

1. In EFT Administrator select the **Server** tab. You should be connected to the server.
2. Select the **Server Options** tab.
3. Below the **Log file format** list, select one of the following: **Never**, **Daily**, **Weekly**, or **Monthly**.
4. Select **Apply**.

Note:
Logs are not written to disk in real-time. As events occur, the server buffers those events in real-time and then flushes (writes) them to file once either a) 60 lines are available, or b) 32kb of log data is received in 1 second or less.

Remote administration

To connect to EFT Server from a remote EFT Administrator you must:

- Configure the EFT Server. This must be done locally on the server.
- Configure the remote EFT Administrator.
- Connect from the remote EFT Administrator

Note:
To reconnect, start, or stop the EFT Server service from a remote location, the remote computer must have a user account on the EFT Server computer with the appropriate administrative privileges.

Configure EFT Server for remote administration

1. Launch the EFT Administrator on the EFT Server computer and connect to the server you want to configure for remote administration.
2. Select the **Remote Administration** tab in the right-hand workspace.
3. Select an IP address from the **Administrator home IP** list. You can select a specific IP or all incoming IPs.
4. Select the **Administrator port**. 1100 is the default port.
5. Select the **Allow remote administration** check box. A warning appears advising you to connect over SSL for more secure administration.
6. Select **Yes** to set up secure administration, or **No** to administer over a clear connection.
7. Select **Apply.** If you chose to use SSL you must create or designate an SSL certificate to use for connections.
8. Close the EFT Administrator. Make sure that the server service is still running (from the control panel service applet).

Configure the remote EFT Administrator

1. Launch the EFT Administrator on the remote computer.
2. Select the **Server** tab in the left-hand pane.
3. Select the Server Group you want to add the remote server to.
4. From the **File** menu, select **Add New FTP Server**. The **Add New Server** dialog appears.
5. Enter the name of the server you want to connect to.
6. Choose **Remote host**.
7. Enter the IP address of the Server in the **Host** field.
8. Enter the port number of the EFT Server you are connecting to In the **Port** field.
9. Select **Save**.

Configuring secure remote administration

To configure secure remote administration, first configure the server to allow remote administration. Create or acquire an SSL certificate, and then consider whether you need implicit or explicit SSL.

Once engaged, SSL encrypts all of your remote administration sessions.

To enable SSL during remote administration

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right-hand pane, select the **Remote Administration** tab.
4. Select the **Use SSL for remote administration** check box.
5. Choose the location of the **Certificate file path** and the **Private key file path** with the browse button depicted by a folder.
7. Enter the **Private key passphrase**.
8. Select **Apply**.

Note:
If you do not already have a certificate and you are administering a local server, you can create a certificate using the **Certificate Creation Wizard** located on the menu bar under **Tools**.

You cannot use the **Certificate Creation Wizard** to create a certificate for a remote server. If you need to create a certificate for a remote machine, you must open the EFT Administrator and use the **Certificate Creation Wizard** locally on that machine.

If you set up secure administration over an SSL connection, you will not be able to use the COM interface from remote machines.

Controlling access by IP address

By default, all IP addresses are granted access to the server. Enhanced File Transfer gives you two ways to limit which IP addresses can connect to your site:

- Grant access to only one specific IP address or a range of IP addresses.
- Deny access to one specific address or a range of addresses.

To grant access by IP Address

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.

2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **IP Access** tab.
4. Select the **Denied Access** radio button.
5. Click the **Add** button. The **IP Mask** dialog box will appear.
6. Enter the IP address or range of IP addresses that WILL have access to your FTP site. EFT Server allows wildcards to select ranges of IP addresses.
7. Select **OK**. The **IP Mask** window disappears.
8. Select **Apply**.

To deny access by IP address

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **IP Access** tab.
4. Select the **Grant Access** radio button.
5. Select the **Add** button. The **IP Mask** window appears.
6. Enter the IP address or range of IP addresses that will *not* have access to your FTP site. **Enhanced File Transfer Server** allows wildcards to select IP address ranges.
7. Select **OK**. The **IP Mask** window closes.
8. Select **Apply**.

Configuring SMTP email notification

You can configure the server to send email alerts whenever certain events occur. You must provide **EFT Server** with the address for an outgoing mail server, an address for the administrator, and other details.

To set up the server to send email notifications

1. Select the **Server tab** in EFT Administrator and select a server the server you want to configure.
2. Select the **SMTP Configuration** tab from the right-hand workspace.
3. In **SMTP Server Address**, enter the address of the mail server the EFT Server will use to send outgoing messages.
4. In **SMTP Server Port**, enter the port number where the mail server accepts messages. The standard is **25**.

5. If EFT Server can connect to the mail server without a log in, leave the **Server requires authorization** check box clear and skip to step ten. If the mail server requires a user name and password from the EFT Server computer, select the **Server requires authorization** check box and continue with step eight.
6. In the **Login** box, enter the user name needed to connect to the mail server.
7. In the **Password** box, enter the password needed to connect to the mail server.
8. In the **Name** box of the **Send Messages FROM** group, enter any name you would like for the "From Name" field.
9. In the **Address** box of the **Send Messages FROM** group, enter any address you would like for the "From Address" field.
10. In the **Name** box of the **Send Messages TO** group, enter the name of the server administrator, or any name you wish.
11. In the **Address** box of the **Send Messages TO** group, enter the email address of the person that should be notified of server events.
12. Select **Apply**.

Note:
The first name/address pair entered is automatically entered into the "To:" field in the send email notification action dialog. Subsequent name/address pairs are automatically entered into the "CC:" field in the send email notification action dialog.

Server statistics

To monitor current statistics at the server, site and user level

1. In the EFT Administrator, connect to the server and select the **Status** tab.
2. In the left pane, select the server, site, or connected user to view the related statistics.

Note:
After selecting a user in the left window, you can use the **Kick User** button below the right window in order to disconnect a user from a site. This does not disable the user, but stops unacceptable activities while you reconfigure the user's access.

Copying a server configuration to several computers

If you are installing Enhanced File Transfer Server on several different computers, and want to create a standard configuration for all machines, install the software on one machine to create a prototype configuration.

Installation and deployment considerations

- The prototype site **Administrator Home IP** must be set to **All Incoming**. It must not be bound to a specific IP address.
- Make sure the destination computers' installation paths are the same as the installation path on the prototype computer.

Deploy duplicate configurations

Set up the deployment configuration

1. Install and register Enhanced File Transfer Server.
2. Configure as desired. This includes passwords, sites, users, all site options, and all user options.

Note:
The configuration process also creates a specific VFS folder structure. Document this folder structure as needed to recreate it on the destination machine.

3. Stop the EFT Server service.
4. Copy the following files from the **EFT Server** program folder (perhaps in a zip file; the delivery method is up to you):
   - FTP.cfg
   - [YourSite].aud

Deploy the configuration to other servers/administrators

1. Create the same folder structure on the destination machine(s) as the folder structure created by the configuration of the prototype machine. The easiest way to do this is to simply copy the FTP folder structure from the prototype to the destination machines.
2. Install and register EFT Server.
3. Cancel the automatic site setup wizard that appears the first time you run the Administrator Interface.
4. Stop the **EFT Server** service and close the Administrator Interface.
5. Paste the files gathered from the prototype computer into the **EFT Server** program folder, overwriting existing files as necessary (which should only be the FTP.cfg file at this point).
6. Restart EFT Administrator. This starts the service.
7. Double-check server and site configuration, and make customizations as necessary. At this point, you should be fully set up on the destination computer.

Connection problems

If you are having problems connecting, check to make sure that:

- Your Username and Password are correct. These are case sensitive.
- The Host (the IP address) and Port are correct.
- The service is running.

> **Note:**
> If the service is not running, you may be able to start the service remotely by configuring Transfer Engine Service Settings located at Edit > Service Applet Settings.

- The network connection is functioning.

Server security considerations

Storing your login and password name may be convenient, but it is not secure. The password is available to anyone who uses the server machine.

Changing the administrator password and port is a good option if you do encounter a security breach.

> **Note:**
> It is so easy to configure the server that many administrators do not give careful consideration to administrative password or port changes. If you do not remember your password and port, you will not be able to connect to the server.

You may encounter port conflicts while attempting to run two sites with implicit SSL encryption. Keep this in mind as you configure multiple sites' encryption options.

Carefully consider inheritance as you begin to grant folder access to different VFS groups. Creating virtual folders gives users access to all subfolders of the folder you point towards.

Setting VFS access with patterns of inheritance derived from parent folders in a logical manner ensures that permission groups have predictable access to folders.

Connection monitoring

EFT Sever can monitor user connections in real time, and record activity to a log.

To monitor a user connection:

1. In EFT Administrator, select the **Status** tab. You should be connected to the server.
2. Select the **Server > Site > user connection** you want to monitor.
3. Select the **Monitor User** button on the bottom toolbar. The connection activities display in the bottom right pane. You can set the number of lines the log records (**Log Scrollback**) and toggle automatic scrolling on or off (**Auto Scroll**).

6

Sites

Creating sites

Enhanced File Transfer Server allows you to create and run multiple sites through a single EFT server. Each site must connect to a separate IP address or port or both. When you create a new site, the New Site Creation Wizard sets up the new site with FTP access enabled. Once you have finished the Site Creation process you can configure the protocols settings for the Site, such as FTP, FTP over SSL, HTTP, HTTPS, and SFTP.

To create a new Site

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Server where you want the new site.
3. Choose **Configuration > Create New Site** from the menu. The **Create New Site** window appears.
4. Enter a **Name** for the site.
5. Choose a **Listening IP** address for the site from the drop-down box or select **All incoming**.
6. Choose a **Port**. The default port used for FTP connections is **21**, however, you can enter any value between 1 and 65,535. If you are setting up the site for HTTP or Secure FTP Connections, you can later turn off plain FTP access in the **Connection Options** tab.

> **Note:**
> Assigning port numbers under 1024 may lead to conflicts with other programs running on your computer.

6. If you want the site to start immediately, select **Start site automatically after creation**.
7. Select the authentication method. The default method is GlobalSCAPE EFT Server Authentication. If you need to use NT authentication see Creating a site that uses NT authentication. For ODBC authentication, see Creating a site that uses ODBC authentication. For LDAP authentication, see Using a LDAP database for authentication.
8. Select **Next**.
9. Enter a path to store the user database. Leave the default path unless you want to store the authentication database in a new location.

10. Select a polling option from the **User list refresh interval** pulldown menu. This selects how often the server checks the database for new users.
11. Select **Next**.
12. Enter a path to the root folder for the site.
13. Select **Create standard subfolders...** to automatically create **Bin**, **Pub**, **Usr** and **Incoming** folders with appropriate permissions under the root folder. This is only necessary if you are trying to mimic a typical default *nix EFT server setup.
14. Select **Enable anonymous access to the server...** to create an anonymous account that does not require a password. The account will have limited permissions.
15. Select **Auto assign home folders to site users** to automatically create a user folder under \Site Root\Usr\[username] when a new user is added.
16. Select **Finish**. If the root folder has not already been created, you are prompted to do so: Select **Yes**. The folder is created and the **Create New Site** wizard closes.

Starting Sites with the server running

To start Sites

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select **Go** from the toolbar. A pulldown menu appears.
3. Select the Site you want to start from the pulldown menu. To start all of them, select **All Sites**.

Stopping sites with the server running

To stop Sites

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select **Stop** from the toolbar. A pulldown menu appears.
3. Select the Site you want to stop from the pulldown menu. To stop all of them, select **All Sites**.

Note:
If you stop a Site while users are connected, the users will be disconnected and file transfers may be interrupted.

Site Options

Changing a site's root folder

The site root folder is specified when you create a new site. However you can later change a site's root folder.

WARNING:
If you change a Site's root folder, all previously configured user and group folder permissions related to that site are deleted.

To change the Site root folder

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Site Options** tab.
4. In the **Site root folder** box, type the path or click the yellow folder button to choose a new Site root folder. This will be a physical folder.
5. Select **Apply**.

Note:
When a connection is established using HTTP, the client (web browser or other HTTP client) shows the root folder, not the user's home folder. This is a limitation of the HTTP protocol.

Creating a site that uses NT authentication

Enhanced File Transfer Server can create sites using the NT user authentication database so users can connect to the site with their NT user name and password. Permissions are assigned to users from the NT User Database on the domain of the system that is running the server. Enhanced File Transfer Server queries the Primary Domain Controller (PDC) for your domain and adds all domain users.

Users are listed as soon as you open the site you created using NT Authentication. You cannot add or change users from Enhanced File Transfer Server, but you can change their permissions, settings and status on the server.

Warning:
NT Authentication transmits passwords over the network without data encryption. To avoid exposing your passwords to possible theft, use SSL connections with NT Authentication.

To create a site

1. Follow steps 1-11 of Creating Sites.
2. In the **Authentication method** list, Choose **Windows NT Authentication**.
3. Click **Next**.
4. Click **Yes**. The **Authentication Options** window opens.
5. Choose **Active Directory (AD) Authentication**, or **NTLM Authentication** to match what is used on the server's domain.
6. In the **Domain Context** section, choose **Use default** if you want to use the authentication database from the machine's current domain, or choose **Custom**, and supply the domain name which has the authentication database you want.
7. In the **Allow access to the following group** section, choose **Everyone** to allow access to every user in the domain's database, or choose **Custom** and supply a group name for users that will have access to the server.
8. In the **User list refresh interval** list, select how often you want GlobalSCAPE EFT Server to check the authentication database for new users.
9. Click **Next**.
10. Enter a path to the root folder for the site.
11. Select **Create standard subfolders...** to automatically create **Bin**, **Pub**, **Usr** and **Incoming** folders with appropriate permissions under the root folder. This is only necessary if you are trying to mimic a typical default *nix EFT server setup.
12. Select **Enable anonymous access to the server...** to create an anonymous account that does not require a password. The account will have limited permissions.
13. Select **Auto assign home folders to site users** to automatically create a user folder under \Site Root\Usr\[username] when a new user is added.
14. Select **Finish**. If the root folder has not already been created, you are prompted to do so: Select **Yes**. The folder is created and the **Create New Site** wizard closes.

Creating a site that uses ODBC authentication

Enhanced File Transfer Server can create sites that use an ODBC database for authentication.

To create ODBC database authenticating site

1. Follow steps 1-11 under Creating Sites.
2. In the **Authentication method** list, choose **ODBC Authentication**.
3. Click **Next**. The **Authentication Options** window opens.

4. In the **Please specify user database data source** box, type a connection string for the ODBC database.
5. Select the **Encrypt passwords** check box to encrypt passwords stored in the database.
6. In the **User list refresh interval** list, select how often you want **EFT Server** to check the database for new users.
7. Click **Next**.
8. Enter a path to the root folder for the site.
9. Select **Create standard subfolders...** to automatically create **Bin**, **Pub**, **Usr** and **Incoming** folders with appropriate permissions under the root folder. This is only necessary if you are trying to mimic a typical default *nix EFT server setup.
10. Select **Enable anonymous access to the server...** to create an anonymous account that does not require a password. The account will have limited permissions.
11. Select **Auto assign home folders to site users** to automatically create a user folder under \Site Root\Usr\[username] when a new user is added.
12. Select **Finish**. If the root folder has not already been created, you are prompted to do so: Select **Yes**. The folder is created and the **Create New Site** wizard closes.

Specifying a PASV IP or PASV port range

If the EFT Server is behind a firewall or NAT device, you may need to specify the Server's IP address or range of ports the server chooses from when issuing IP:PORT information to clients.

To specify a PASV connection through a range of ports

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Site Options** tab.
4. Select **Assign PASV mode IP Address**.
5. In the **IP** box, enter the server's IP address as should be seen by those outside your network.

Note:
Usually applies under SSL sessions when the NAT or FW device cannot see and therefore properly map the internal IP address of the server. Also applies if the NAT or FW device is misconfigured. It is recommend you first try connecting to the server with this field left as is.

6. In the **Port Range** boxes, enter the range of ports the server uses for PASV connections.

Note:
User primarily to limit the amount of ports used for the data connection portion of the FTP session, especially when the FW or NAT device was configured to only allow traffic on certain ports.

7. Select **Apply**.

Note:
If you specify a PASV mode port range you must open the same range of ports on your firewall.

Allow user name and password replacement variables

User name and password variables are used by Event Rules to use a single event rule to support multiple users with a copy/move action. This allows the server to store user name and password variables in memory during client sessions. You can enable or disable this feature at the site level. The default is disabled. For more information on using this in an event rule, see Copy/Move Event Action.

To allow user name and password replacement variables

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right-hand pane, select the **Site Options** tab.
4. Select **Allow username/password replacement variables for Event Rules by storing these values in memory for the duration of a client session**. A security vulnerability warning appears.
5. Select **Yes**.
6. Select **Apply**.

Note:
Allowing user name and password replacement variables introduces a potential security vulnerability in that it allows passwords to reside in memory on the server. The risk is small, but it should be avoided unless you require the variables for an event rule.

Blocking site-to-site transfers

Although site-to-site transfers are great for the user, expediting what otherwise could be a slow transfer, many administrators consider site-to-site transfers a security risk, exposing servers to "port theft" or "FTPing by proxy" attacks. Depending on how your servers are configured, you may want to block these types of transfers.

To allow or not allow site-to-site transfers

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Site Options** tab.
4. Select or clear the **Block site-to-site transfers** check box.
5. Select **Apply**.

Blocking anti-timeout schemes

Enable blocking of anti-timeout schemes to defeat FTP clients that send a series of random commands to maintain an unattended connection to EFT Server.

To automatically disconnect idle users using anti-timeout schemes

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Site Options** tab.
4. Select the **Block anti-timeout schemes** check box.
5. Select **Apply**.

Modifying messages

EFT Server can display messages to users in the following situations:

- Successful connection
- Login (under User settings)
- Maximum connections exceeded
- Exit

Connection Message

The connection message appears when a user first connects, but before a user logs on.

To modify the Connection message

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, click the **Site Messages** tab.
4. In the **Connect message** box, enter the text that you want to appear when the user connects.
5. Select **Apply**.

Login Message

Login messages may be applied at the User or User Setting Level. Users automatically inherit the message applied to their User Setting Level. You can optionally display a message unique to a User.

To modify the login message for a User or User Setting Level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User Settings you want to configure from the left-hand navigation tree.
3. Select the **Main** tab.
4. In the **Login message list,** choose an option.

- **Use Default**. You cannot add an additional message when a user connects. The default message for a successful login is:

```
230-Login OK. Proceed.
```

- **Add to Default**. This option places the default message on one line, then adds the message you typed into **Login message**. For users, the message set at the User Setting Level is the default.
- **Replace Default**. The server does not display the default message, but displays the message you type in to the Login message box. For users, the message is defaulted at the User Setting Level.
- **None**. No messages appear when a user logs in.

5. Select **Apply**.

Maximum Connections Message

You can configure a site to only allow a specified number of maximum simultaneous connections. If you choose this option, you can specify a message for users when the maximum simultaneous connections number is exceeded.

To Modify the Maximum Connections Message

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, click the **Site Messages** tab.
4. In **User limit message**, enter the message you wish to display if the maximum simultaneous connections number is exceeded.
5. Select **Apply**.

Exit Messages

The server can send an exit message when the client closes the session gracefully by using the FTP QUIT command.

To modify the exit message

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.

2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Site Messages** tab.
4. In the **Exit message** box, enter the exit message you wish to display.
5. Select **Apply**.

Allow HTTP transfers

To enable HTTP transfers at the site level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Connection Options** tab.
4. Select **Allow HTTP Transfers on Port**. The default port number is 80.
5. Select **Apply** to save and implement the changes.

Note:
For a user to access EFT using HTTP, **Allow access using HTTP protocol** must be selected at the user or user setting level.

Setting Transfer Protocol Security

SSL

Enabling FTPS, HTTPS, (SSL) at the site level

Enhanced File Transfer Server has robust SSL configurations that allow you to configure SSL connections on all sites, at the site level, at the user setting level, or at the user level. You can also configure SSL with a combination of these four levels. In order for SSL support to be available at any level it must first be configured at the site level.

To enable SSL at the site level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Connection Options** tab.
4. Select **Enable FTP access** to allow both standard FTP connections and SSL connections. Clear **Enable FTP access** to allow only SSL connections to the site.

Note:
If you clear **Enable FTP access**, you must enable one or more of the other connection options or no one will be able to connect to the site.

5. Select **Allow HTTPS transfers** to allow SSL connections over HTTPS. Select the port for HTTPS. The default is 443.
6. Select:
   - **Enable explicit SSL connections**,
   - **Enable implicit SSL connections**,
   - Both.
   - Neither.

Note:
If Enable implicit SSL connections is selected you can change the Implicit SSL port. The default port is 990, which is normally used by FTP clients that support implicit SSL.

7. Select the SSL Compatibility. If you want to allow the user to use any compatible SSl flavor, leave **Auto Negotiable** selected. If you want to force a particular flavor (TLS 1.0, SSL 2.0, or SSL 3.0), select it, and only that flavor is allowed.
8. Select the **Certificate** and **Private Key** file paths. If you used the **Create SSL Certificate Wizard** and selected the **Set up Server to use the generated certificate** check box, then the **Certificate** and **Private Key** file paths will already be completed. Otherwise, choose the files using the browse buttons.
9. Enter the **Private Key Passphrase**. This is the passphrase that was used when the certificate was created. An incorrect passphrase generates errors when you select **Apply**.
10. Select **Require certificates from connecting clients**.

    If **Require certificates from connecting clients** is not selected, then clients that support SSL can connect to the server without supplying a certificate. If this box is selected, then FTP clients requesting an SSL connection must present a certificate before the server will allow them to connect. The client certificate must be in the Trusted Certificates database or signed by a certificate in the Trusted Certificates database. If the client has a certificate that does not meet those conditions, the connection is denied. However, its certificate is placed in the Pending Certificates database, where it can later be added to the Trusted Certificate Database. If the client does not present a certificate, the connection is denied.

Disabling SSL connections

You can disable SSL support for every user on the server by disabling SSL support at the site level, or you can disable SSL for a specific user or User Setting Level.

To disable SSL connections for a site on the server

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.

2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right-hand pane select the **Connection Options** tab.
4. Select **Enable FTP access** and enter the port.
5. Clear BOTH **Enable explicit SSL connection**, and **Enable implicit SSL connection**.
6. Select **Apply.**

Note:
If SSL connections are disabled at the site level, they are also disabled for all User Setting Levels and users on the site.

To disable SSL connections for a user or User Setting Level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right-hand pane, select the **Security** tab.
4. Select **Allow access using FTP protocol**.
5. Toggle **Allow access using SSL over FTP protocol** until it is empty and white.
6. Select **Apply.**

Creating certificates

A certificate on the client must be associated with the server in order to initiate an SSL connection. When you are administering the server on the local machine, you may create certificates using the **Certificate Creation Wizard** (**Tools > Certificate Creation Wizard**) or import your own. There are three types of files associated with an SSL certificate key pair:

Private key file (.key) - The private key should never be distributed to anyone. It is used to decrypt the session which is encrypted by the public key.

Certificate request file (.csr) - Each time you create a certificate using GlobalSCAPE EFT Server a Certificate request file is also created. This file can be signed by GlobalSCAPE EFT Server's **Certificate Signing Utility** or sent to intermediate certificate authority such as GeoTrust for signing.

Certificate file (.crt) - This is a signed certificate, whether self-signed or signed by an intermediate certificate authority.

The private key (.key) and certificate request (.csr) files are created at the same time. You are prohibited from creating certificates for the EFT Server while remotely administering the server because this action can create a security breach. Any certificates you create while remotely administering remain on the remote machine unless you take special steps to deliver and associate these files with the local machine.

To create an SSL certificate

1. On **EFT Server**'s menu bar, choose **Tools > Certificate Creation Wizard**. The certificate wizard appears.
2. Enter the **Certificate Name**. Name the certificate that will be generated by the **Certificate Wizard**.
3. Enter the **Output Location.** Enter the path or browse to the folder where the certificate is kept. The wizard saves the .key, .csr, and .crt files to the location you enter here.

> **Note:**
> If you are purchasing a signed certificate from a certificate authority (CA), you usually need to open the certificate request file (.csr) and copy the contents to forward them to the CA. To do this, locate the .csr and open it with Notepad; then you can copy and paste the contents.

4. Choose the **Expiration Date**. Define how long the certificate remains valid.
5. Enter and confirm the **Passphrase**. Determine the passphrase that is used to encrypt the private key. The passphrase can be any combination of characters or spaces. Do not lose the passphrase. The certificate is useless without it.
6. Choose a **Key Length (in bits)**. Choose 512, 1024, 2048, or 4096 bit keys. Smaller keys are faster, larger keys are more secure.
7. Select **Next**.
8. Enter the **City/Town** where your organization is located.
9. Enter the **State/Province** where your organization is located.
10. Enter the name of your **Organization**.
11. Enter the **Common Name**. This is typically your name or the domain name associated with the site.
12. Enter a valid **E-Mail** address.
13. Enter a **Unit** name. Typically you enter a department or branch name.
14. Enter the two-digit **Country** code that identifies the country where your organization is located.
15. Select **Next**.
16. If **Use this certificate for Server authentication** is cleared, the wizard saves only the certificate files in the folder you previously specified. If selected, the wizard associates the certificate to the administration service or a site(s) you specify.

> **Note:**
> Associating a new certificate with a site requires a restart of the site, and any active users will be disconnected. We recommend that you associate certificates when sites are inactive or stopped.

17. If **Add this certificate to the Server Trusted Certificate list** is selected, the wizard adds the certificate to the Trusted Certificates database. Use this feature if you are creating certificates for user distribution. You can limit server access to include just

the users that have the certificate. You can verify the addition to the Trusted Certificate Database by selecting **Tools > Certificate Manager**.

18. Use **the Apply certificate to** pull down menu to choose which components of the server are affected.
19. Select **Finish**.

Selecting a certificate

To assign a certificate you have created or obtained to a site

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Connection Options** tab.
4. Select **Enable explicit SSL connection** check box or the **Enable implicit SSL connection** check box or both.
5. Select the certificate file by clicking the browse button next to the **Certificate file path**.
6. Select the private key by clicking the browse button next to the **Private Key file path**.
7. Enter the **Private Key Passphrase**. The passphrase must match the passphrase that was used when creating the certificate.
8. Select **Apply**.

Signing a certificate

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

To sign a certificate request

1. Obtain the Certificate Signing Request file (.csr). This can be done through email or any other file delivery method.
2. Choose **Tools > Certificate Signing Utility** from the menu. The **Sign Certificate Request** dialog appears.
3. **Client certificate request -** Click the folder to browse and select the Certificate Signing Request (.csr) file you want to sign.
4. **Output client certificate -** Browse and choose a folder in which to save the signed certificate (.crt) file.

5. **Server certificate -** Browse and choose the certificate you will sign with. This certificate must be in your trusted certificate database in order for clients submitting the signed certificate to connect to the site.
6. **Server private key** - Browse and select the private key file (.key) associated with the server certificate.
7. Enter the **Passphrase** associated with the server certificate.
8. Choose an **Expiration date**.
9. Select **OK**. The new certificate is saved in the folder you selected.
10. Return the certificate file (.crt) to the user.

Trusted certificates

If you require certificates from connecting clients before they can connect, then their certificate must be in the Trusted Certificates Database or signed by a certificate in the Trusted Certificate Database. To manage trusted certificates, select **Tools > Certificate Manager** from the menu.

Importing a certificate into the Trusted Certificate Database

1. On the menu bar, choose **Tools > Certificate Manager**. The **Certificate Manager** appears.
2. Select **Import** on the bottom of the **Trusted Certificates** window.
3. Browse to the folder that contains the client's certificate file and select the file.

Note:
Enhanced File Transfer Server can import a digital certificate from the following formats: PEM, Base64 Encoded X509, DER Encoded X509, PKCS#7, PKCS#12.
The Private Key associated with the digital certificate must be in one of the following formats: PEM, DER, PKCS#8, PKCS#12.

4. Select **Open**.
   - Enhanced File Transfer Server automatically detect the certificate format. If it an informative error message will appear.
   - If Enhanced File Transfer Server is unable to determine the format, or if the import fails, you can manually convert a digital certificate to one of the above formats and import it. Consult the distributor/vendor of your certificate for details on this process.
5. The certificate is added to the Trusted Certificates database. Clients submitting that certificate are now able to connect to the server.

Exporting a certificate from the Trusted Certificate Database

1. Select **Tools > Certificate Manager** from the menu. The **Certificate Manager** window appears.
2. Select **Export**.
3. Browse to the folder where you want to save the certificate file.
4. Enter a name for the certificate file.
5. Select **Save**.

Importing certificates from Microsoft IIS 5

To use a certificate that you are using in IIS 5 you must:

- Add a Certificate Snap-in to your Microsoft Management Console,
- Export the certificate from IIS 5, then
- Import the certificate into Enhanced File Transfer Server.

Add the Certificate Snap-in

1. On the computer containing the certificate you want, select **Start**, then **Run**, and then type mmc to open the **Microsoft Management Console**.
2. On the Console menu, select **Add/Remove Snap-in**... from the console menu.
3. Select **Add**. The **Add Standalone Snap-in** dialog appears.
4. Select Certificates from the list and then select **Add**.
5. Select **Computer account**, then **Next**.
6. Select **Local computer**, then **Finished**.
7. **Close** the **Add Standalone Snap-in** dialog.
8. Select **OK** on the **Add/Remove Snap-in** dialog.

Export the certificate from IIS 5

1. Under the **Tree** tab in the **Microsoft Management Console** expand **Certificates**.
2. Select the **Personal** folder and then the certificate you want to export.
3. On the **Action** menu select **All Tasks>Export**…
4. Select **Next**.
5. Select **Yes**, export the private key, then select **Next**.
6. Select **Personal Information Exchange – PKCS #12 (.PFX)** and then select **Next**.
7. Enter the password you used when you created the certificate and select **Next**. This will create a .pfx file.

Import the certificate into Enhanced File Transfer Server

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Connection Options** tab.
4. Select **Enable explicit SSL access**, **Enable implicit SSL access**, or select both.
5. Select the yellow folder next to **Certificate file path** to browse and select the .pfx file you created in Export the certificate from IIS 5.
6. Select the yellow folder next to **Private key file path** to browse and select the .pfx file you created in Export the certificate from IIS 5.
7. Enter the password you used when you created your certificate in **Private key Passphrase**.
8. Select **Apply**. A message appears prompting a site restart.
9. Select **Stop** from the toolbar, stop the site, wait for the site to stop.
10. Select **Go** from the toolbar to restart the site.

SFTP

Enabling SFTP

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Connection Options** tab.
4. Select **Enable SFTP (SSH2) access**. If you have not already done so, a dialog box prompts you to create a server key. Select **Yes**. The SFTP Settings tab appears.
5. Create a Site key pair.

To create a Site key pair

1. Select **Create** next to the site key pair field. A **Create SSH2 Public/Private Keypair** window appears.
2. Enter a name for the key pair and select the location to store it. Select **Finish**. Enhanced File Transfer Server generates and stores the key pair.

Select algorithms

1. In the **Use encryption algorithms** list, select any or all algorithms you want to allow for encrypting SFTP sessions. Hold down the **Shift** key on your keyboard to select a series, or hold down the **CTRL** key to select several that are non-contiguous.
2. In the **Use MAC algorithms** list, select any or all the algorithms to allow their use for message authentication. Hold down the **Shift** key on your keyboard to select a series, or hold down the **CTRL** key to select several that are non-contiguous.

3. Select **Apply**. A message appears telling you the site must be restarted for the changes to take effect.
4. Select **Yes**.
5. IF you want to change the SFTP port return to the Connection Options tab and specify the port number next to **Enable SFTP (SSH2) access on port.** 22 is the standard port for the SFTP protocol.

SFTP Transport layer settings

To select Message Authentication Codes (MAC)

Message Authentication Codes are algorithms used to confirm data has not been altered between the client and server.

1. In EFT Administrator, select the **Server** tab. You should be connected to the server, and SFTP should be enabled.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **SFTP Settings** tab.
4. In the **Use MAC algorithms** list, choose any or all of the four options:
    - hmac-md5
    - hmac-md5-96
    - hmac-sha1
    - hmac-sha1-96
5. Select **OK**. Enhanced File Transfer Server tries each selected MAC with the client until an algorithm is agreed upon.

SFTP algorithms

To select encryption algorithms (ciphers)

1. In EFT Administrator, select the **Server** tab. You should be connected to the server, and SFTP should be enabled.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **SFTP Settings** tab.
4. From the **Use encryption algorithms** list, select any or all encryption methods.

Encryption algorithms

- **ARCFOUR**: Arcfour is intended to be compatible with the RC4 cipher trademarked by RSA Data Security, makers of the famous OpenPGP program. It uses a 128-bit key and provides good security.

- **cbc** - Cipher Block Chaining is an encryption technique used with block ciphers where the previous encrypted block is used as a basis for encrypting the next block, so that every block has to be in the correct order to be decrypted properly.
- **CAST128**: This cipher is the CAST block cipher using 128 bit keys.
- **Triple DES (3DES)**: This algorithm uses a 24-bit "triple key" to encrypt data 3 times. The 24-bit key is split into 3 8-bit segments and each is used for encryption. Triple DES is fast, but not as strong as the other algorithms.
- **Blowfish**: The Blowfish algorithm is a public-domain block cipher method using a 128-bit key. Blowfish was intended to be a replacement for 3DES. It provides good security.
- **Twofish**: Twofish is an improved version of Blowfish. It provides the strongest security available in GlobalSCAPE EFT Server and should protect your data in most transfers. GlobalSCAPE EFT Server recognizes Twofish encryption using 128 and 256 bit keys.

5. Select **OK**. Enhanced File Transfer Server tries each selected algorithm with the client until one is agreed upon.

Creating client key pairs for SFTP

When clients attempt to create an SFTP connection with your server, the server must send a key to the client verifying its identity. You can create the necessary key with Enhanced File Transfer Server. Use the same key for several sites, or create separate keys for individual sites.

To create a client key pair

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, click the **SFTP Settings** tab.
4. Select the **Enable SFTP** check box.
5. Select **Create**. A **Create SSH2 Public/Private Keypair** window appears.
6. In the **Enter path to store key pair**, enter the path where you want to keep the created key pair. Or select the browse button to navigate to the path where you want to store the key pair.
7. Select **Finish**. A note appears telling you the key pair was created successfully.
8. Select **OK**.

Note:
To use the key for other sites, rather than click Create, in the **Site key pair** box of the **SFTP Settings** tab enter or browse to the path where you stored the key.

Requiring SFTP public key authentication

You can require all users who make SFTP connections to use public key authentication. If you do, the users must send you their public keys, which you must import into **Enhanced File Transfer Server**. You must then set the user account to require public key authentication.

To import public keys

1. Receive a user's public key via email, ftp, or on a disk, etc.
2. Store it on the same machine or network with **Enhanced File Transfer Server**.
3. In EFT Administrator, select the **Server** tab. You should be connected to the server.
4. Select **Tools > SSH Key Manager** from the menu. The **SSH Key Manager** window appears.
5. Select **Import**. The **Open** window appears.
6. In the **Look in** list, select the folder where you stored the public key.
7. Select the public key.
8. Select **Open**. An **Importing key...** window appears.
9. In **Please specify the name for this key**, leave the name as it is, or enter a new name.
10. Select **OK**. The key appears in the **SSH Key Manager** window.
11. Select **OK** again.

To require a user's public key

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.
4. In the **SFTP Settings** section, select the **Require client's public key** check box.
5. In the **Require client's public key** list, select the user's public key.
6. Select **Apply**.

Note:
You can follow the same process and require a public key for an entire User Setting Level, simply select a User Setting Level instead of a user.

If the **Require client's public key** check box appears grayed out, the

user is inheriting the permission or requirement from his User Setting Level.

Allowing SFTP password authentication

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.
4. In the **SFTP Settings** section, clear the **Require client's public key** check box.
5. Select **Apply**.

Note:
If the check box appears grayed out, the user is inheriting the permission or requirement from his User Settings Level.

Advanced

Setting maximum transfer speeds

You can control a user's maximum transfer speeds at three levels:

- The site level
- The user setting level
- The user level

Note:
The Site level sets the limits of the User and User Setting Levels.

To configure maximum transfer speeds at the Site level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Advanced** tab.
4. Select the **Max transfer speed (KB/s)** check box and enter the maximum transfer speed for the site. The server does not set a maximum transfer speed if the box is cleared.
5. Select **Apply**.

To configure maximum transfer speeds at the User and User Setting levels

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.

2. Select the User or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Quota** tab.
4. Select the **Max transfer speed** check box and enter the maximum transfer speed (in Kilobytes per second) for the user.
5. Select **Apply**.

Setting maximum concurrent socket connections to a site

You can set the maximum number of connections to the Server at the site level. With multiple sites, this means that some sites can allow more users than other sites.

To restrict the number of socket connections

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Advanced** tab.
4. Select **Max concurrent socket connections** and enter the maximum number of users you want to allow at any given time. If the box is cleared, the server does not restrict the number of users.
5. Select **Apply**.

Note:
The Max concurrent connection toggle limits the amount of socket, or low level, connections allowed by the server. When this limit is reached, any subsequent connection attempt generates a socket or network error in the client. It reacts as if the server is not even there. This occurs because the server refuses the connection entirely. For a server set up as an anonymous FTP server, it is recommended to limit connections on a per user basis. In this case, this will at least allow the user to partially connect before being told that the server is full or busy—a more graceful way of denying the connection.

Setting maximum concurrent logins

You can set the maximum number of connections to the Server at the site level. With multiple sites, this means that some sites can allow more users than other sites.

To restrict the number of user logins

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.

3. In the right pane, select the **Advanced** tab.
4. Select **Max concurrent logins** and enter the maximum number of logins you want to allow to a user at any given time. If the box is cleared, the server does not restrict the number of users.
5. Select **Apply**.

Setting maximum connections per user

You can set the maximum number of simultaneous connections for a user at three levels;

- The site level
- The user setting level
- The user level

Note:
The site level provides a limit over all other levels (see Overview). For example, if the site level **Max connections per user** is 5, and a user's User level **Max connections per user** is set to 10, the user can still only connect to the server 5 times simultaneously.

To set maximum connections per user at the Site level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Advanced** tab.
4. Select the **Max connections per user** check box and enter a number. If the box is clear a user can create an unlimited number of concurrent connections to the site (or according to the limits defined at the User or User Settings level).
5. Select **Apply**.

To set maximum connections per user account at the User and User Setting Level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Quota** tab.
4. Select the **Max connections per user** check box and enter the maximum times you wish that **User** account or users in that **User Setting Level** to be able to simultaneously connect to the site. Keep in mind that a gray check on a **User** account indicates the account is inheriting parameters from the **User Setting or Site level**.
5. Select **Apply**.

Banning unwanted file types

Enhanced File Transfer Server can block the upload or download of certain files. You can specify which files to block using wildcards or exact file names.

To ban files

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Advanced** tab.
4. Select **Exclude the following files from the site** and enter the filename or wildcard representation (*.mp3 or *.mp?) for the file(s) you want to exclude from the site. If you have more than one entry, separate each with a comma.
5. Select **Apply**.

Assigning a site's IP address and port

A site's IP address is initally specified when it is created.

To change the listening (incoming) IP address

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Site Options** tab.
4. In the **Home IP** list, select the IP address you want for the site.
5. Select **Apply**.

Setting the site port

EFT Server allows you to define a listening port number and IP address for each site. The default for FTP sites is 21, the default for HTTP is port 80, etc. You can enter any value between 1 and 65,535.

Warning:
Assigning a port number under 1024 may lead to conflicts with other programs running on your computer.

To change a Site's listening port

1. In EFT Administrator, select the Server tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Connection Options** tab.

4. Enter the port number in the **FTP Port** box.
5. Select **Apply**.

Disconnecting problem users

Enhanced File Transfer Server employs the following methods to disconnect problem users:

- Blocking anti-timeout schemes
- Disconnecting after a defined number of invalid commands
- Disallowing the NOOP command
- Disabling an account after a defined number of incorrect login attempts
- Setting a maximum idle time limit

To block anti-timeout schemes

Many FTP clients send random commands such as REST 0, PWD, TYPE A, LIST, etc., to an FTP server to keep the session alive while the client is idle. **EFT Server** can attempt to block these schemes.

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Site Options** tab.
4. Select the **Block anti-timeout schemes** check box.
5. Select **Apply**.

To disconnect users after a defined number of invalid commands

The server can automatically disconnect and even ban the IP addresses of users who send an excessive number of invalid commands to the server:

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Advanced** tab.
4. Select **Disconnect user after ___ consecutive invalid commands** and enter the number of invalid commands allowed before you disconnect the user. You may permanently ban the user's IP address from the site by selecting the **Ban IP address after excessive invalid commands** check box. You may later remove the ban on the user by removing their IP address from the list in the site's **IP Access** tab.
5. Select **Apply**.

To allow or disallow the NOOP command

Many FTP clients send a NOOP command to the server during idle times to keep the connection alive. You can choose whether or not to allow the NOOP command. If you disallow the NOOP command it will be considered an invalid command and treated according to your settings under **Disconnect after [Number of] invalid commands**.

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.
4. Select the **Allow NOOP command** check box to allow the NOOP command or clear the **Allow NOOP command** check box to treat the NOOP command as an invalid command.

   Note:
   If you are banning users who send excessive invalid commands and you are also treating NOOP as an invalid command then you will be banning users for sending the NOOP command. You may later remove the ban on the user by removing their IP address from the site's list in the **IP Access** tab. A gray check box in a user account indicates that the account is inheriting parameters from the User Setting Level.

5. Select **Apply**.

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

The server can automatically disable user accounts if users try to connect with the wrong password too many times.

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.
4. Select **Disable account after ___ incorrect password retries** and enter the maximum number of password retries you want to allow in the corresponding box. A gray check box in a User account indicates that the account is inheriting parameters from the User Setting Level.
5. Select **Apply**.

Enabling time out

You can automatically disconnect users after a specified time of inactivity.

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.

2. Select the User or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Quota** tab.
4. In the right pane, click the tab and select the **Enable time out** check box. Enter the maximum allowable seconds of inactivity allowed before the user is disconnected.
5. Select **Apply**.

Flooding and denial of service prevention

You can configure the server to automatically ban IP addresses that may potentially be associated with a DoS (Denial of Service) attack. The server monitors connection patterns, tracks each user's activity density, and then bans IP addresses with unnaturally dense activity.

To activate Auto-ban

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **IP Access** tab.
4. Select a sensitivity level using the slider bar and ban period using the radio buttons based on the following:

    - **Ban IPs for time period proportional to sensitivity (higher = longer)**

        If you select this option, IPs are banned temporarily. The server will restrict this IP's access to the server for a minute or two. The amount of time a user is banned from the site depends on the server security setting you selected using the slider bar. Choosing to ban users temporarily means that if the server makes a mistake and identifies an ordinary, but very active user as a threat, the user will soon be able to reconnect to the FTP site.

        Banning an IP address temporarily protects the server from attacks. If the server is correct and a temporarily banned IP was the source of an attack, the server will not be harmed by the attempted attack. The server's resources will remain free or minimally burdened, instead of being completely bogged down by the attacking IP.

        When you ban IP addresses temporarily, the level of security you set for the slider indicates both the number of seconds the user can attempt to occupy all of the server's resources before being banned and the number of seconds the user will be banned. The higher the security, the shorter the amount of time before the user is banned and the longer the user will remain banned.

    - **Ban IPs permanently (Add to TCP/IP Access restrictions list)**

If you elect to permanently ban the IP addresses of users whose activity fits the pattern of an attack, those users will be immediately banned as soon as they exceed the number of connections allowed for your security level. If the server has banned a user, you will need to modify the TCP/IP Access restrictions list to allow access.

5. Select **Apply**.

OpenPGP

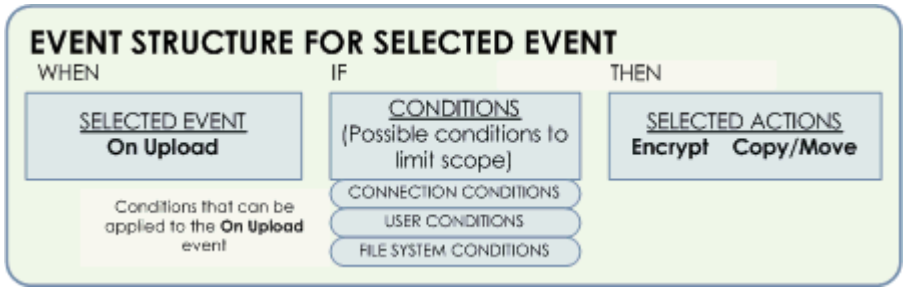
OpenPGP

EFT Server uses OpenPGP (based on the open source implementation of Pretty Good Privacy) technology to safeguard transferred data. The OpenPGP data encryption (or decryption) process is directed by **Event Rules** that specify how data files are treated in a particular context. OpenPGP uses two components, a public key and a private key, to encrypt data and maintain security. These two components are considered a key pair and are associated with a particular Site.

The key pair is stored on the **OpenPGP Key Ring** which is the management tool for public keys and key pairs. The **OpenPGP Key Ring** contains all key information and allows **Import**, **Export**, **Creation** and **Deletion** of keys. The **Settings** function on the OpenPGP key ring permits the user to change or specify a file path for a key.

New key pairs are created using the **OpenPGP Key Generation Wizard**. The wizard prompts you for key parameters and creation of a passphrase. Once the new key pair is generated, the user must determine if the new key pair will be the default for the entire site. Allowing assignment of a default key pair will automatically select this key when configuring an event rule using OpenPGP encryption.

Operation of OpenPGP functions (encrypt, encrypt and sign, and decrypt) are described in the **Event Rules** section. This example shows how a trigger event (**On Upload**) is used to initiate OpenPGP encryption.



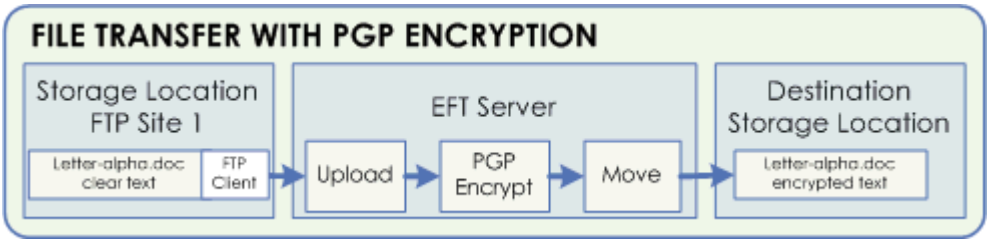
OpenPGP encryption is only available for certain events:

On Upload - when a file is uploaded to a location.

On Rotate Log - when a log file is closed out and a new log initiated.

On Timer - an event that occurs once or according to a schedule.

A simple example of the file transfer process where the EFT server uses OpenPGP to encrypt uploaded data and then the Off-load capabilities of EFT Server to move the file to another location.



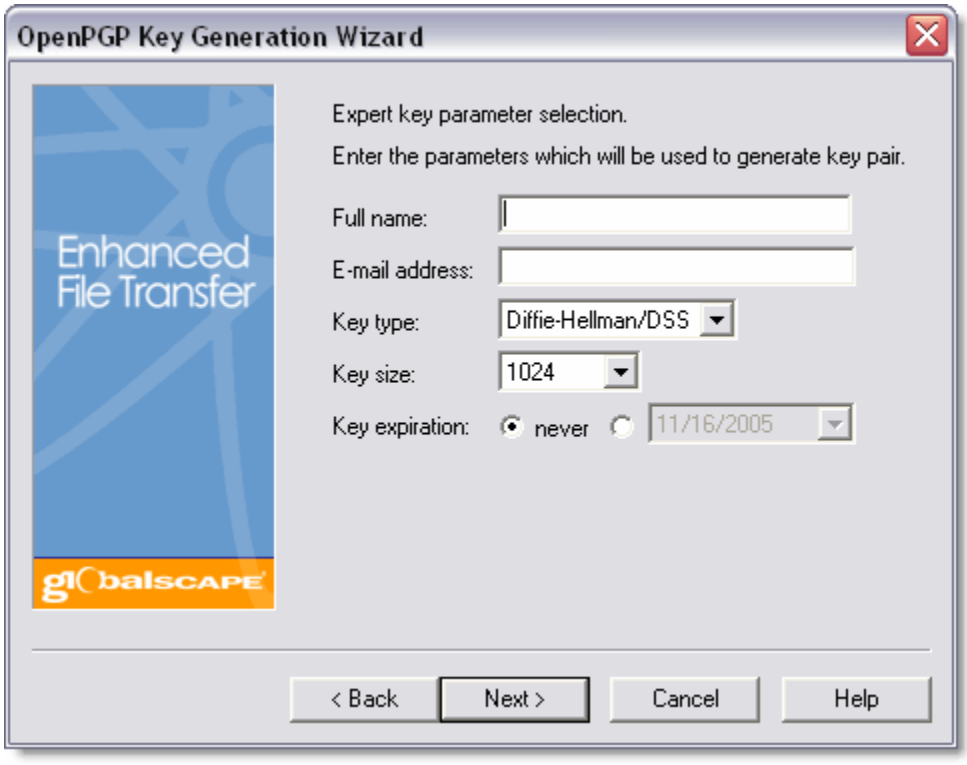
Key creation/deletion

New key pairs for OpenPGP encryption are created using the OpenPGP Key Generation Wizard.

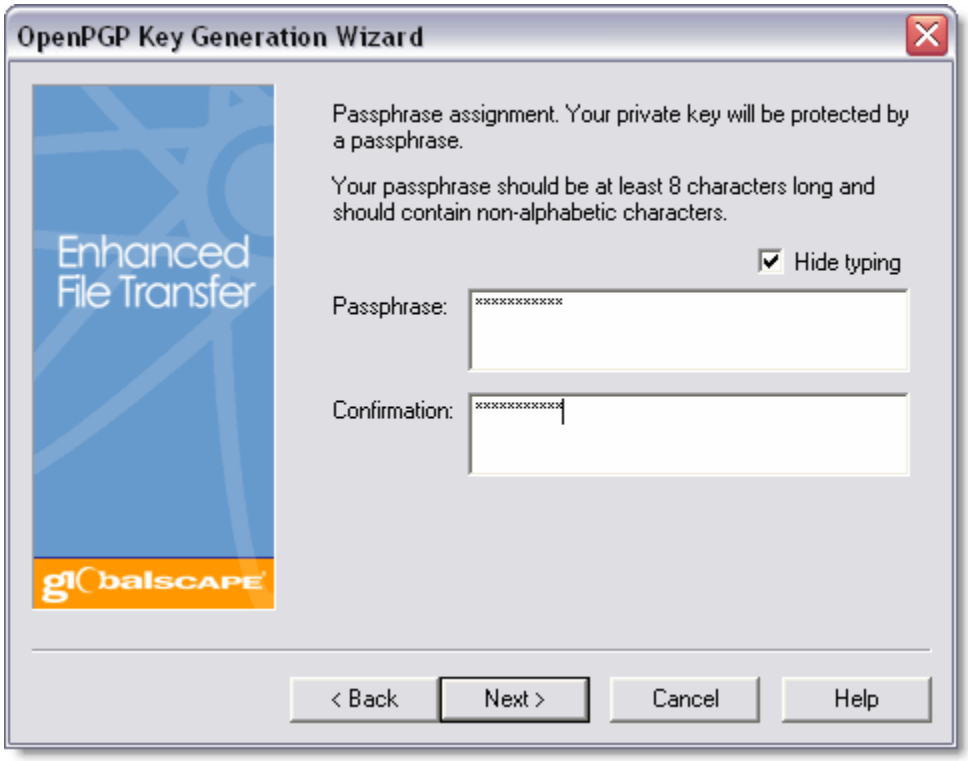
To access the Key Ring Manager and use the OpenPGP Key Generation Wizard

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **OpenPGP Security** tab.
4. Select **Create New Key Pair**. The OpenPGP Key Generation Wizard appears.

5. Read the instructions in the wizard welcome window and select **Next**.



6. Enter the **name** of the site and the relevant **email address**.
7. Select the **Key type**. Select from Diffie-Helman/DSS or RSA.
8. Select the **Key size**. Larger bit sizes increase security, but increase encryption time.
9. Select the **Key expiration** date. This is optional.
10. Select **Next**.

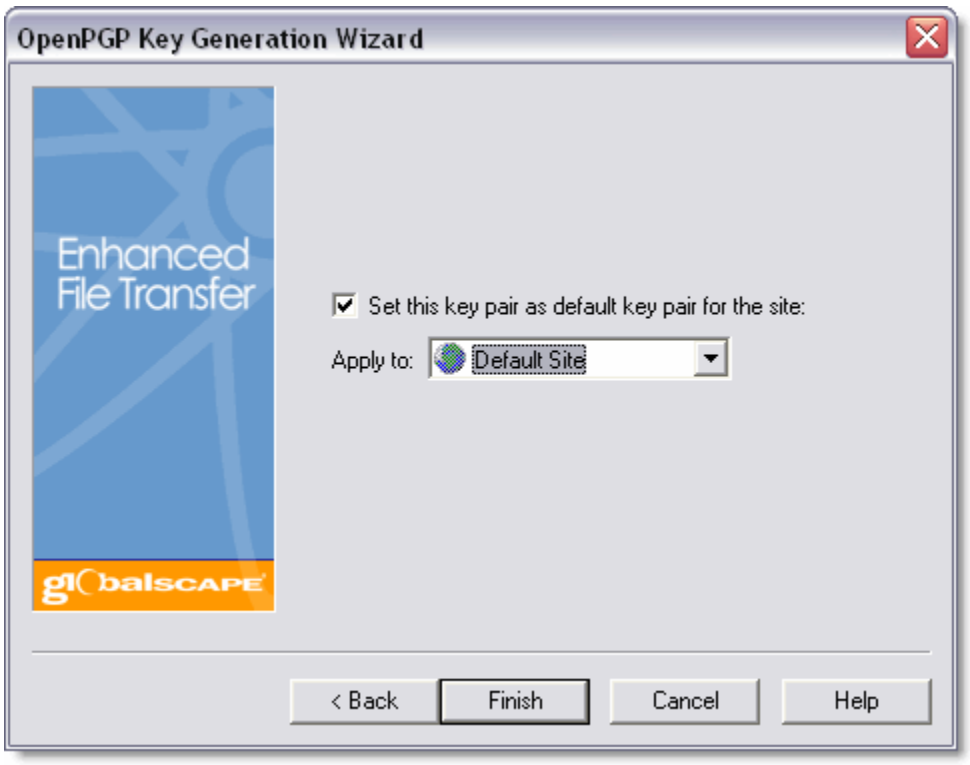


11. Enter your passphrase in the **Passphrase** text box.

> **Note:**
> If **Hide Typing** is checked, the passphase you enter is masked and appears as asterisks.

12. Repeat your passphrase in the **Confirmation** box.
13. Select **Next**.

If the passphrases match key generation begins, otherwise you are prompted to re-enter the passphrase. The passphrase must contain at least 8 characters. Upon successful key generation the final wizard window appears.



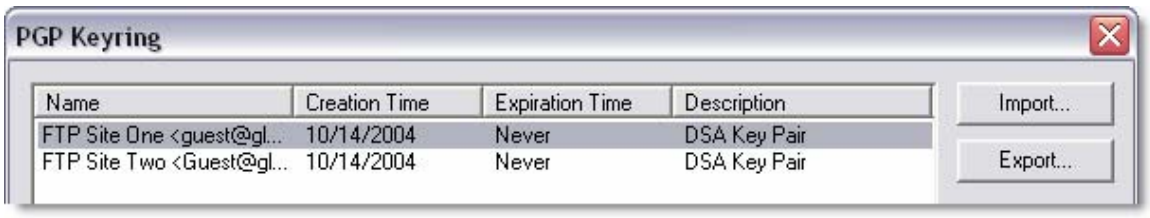
14. Remove the check from **Set this key pair as default key pair for the site** if the key is for a client or you do not wish for this key pair to be the default for the site.
15. Select **Finish** to generate the key pair. A notification window indicates successful generation of the key and addition to the server key ring.
16. Select **OK** to close the notification window.

To delete a key pair

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Secure Storage** tab.
4. In the **OpenPGP Settings** area select **Launch the OpenPGP Key Ring**.
5. Highlight the appropriate key pair and select **Remove**.
6. Select **Yes** in the dialog box to delete the key pair.
7. Select **Close** to exit the **OpenPGP Key Ring Manager**.

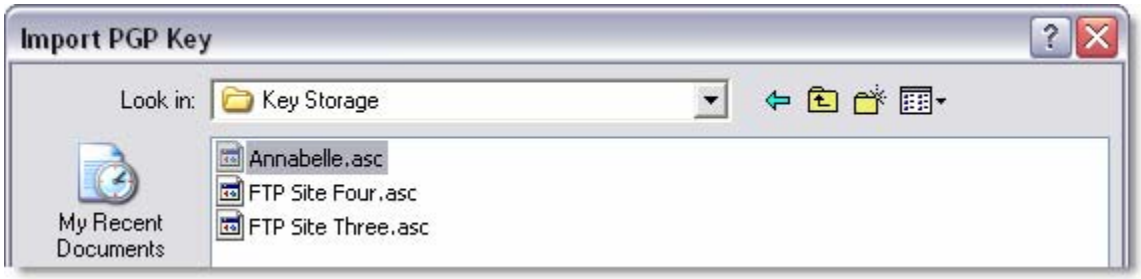
Key import/export

The **OpenPGP Key Ring** can be used to **Import** or **Export** keys.

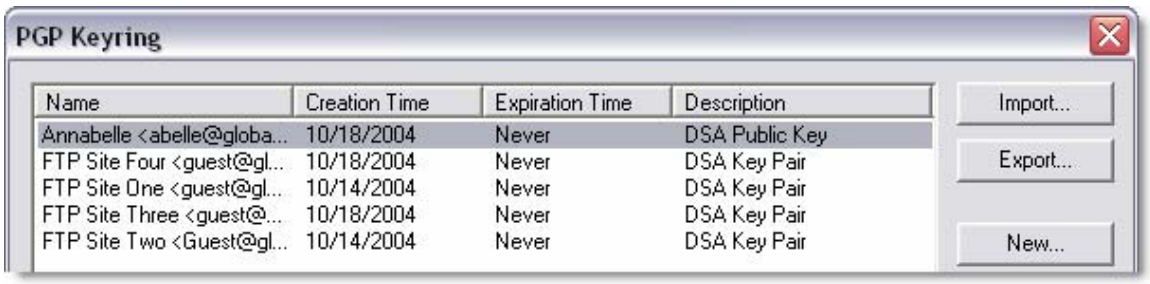


To access the Key Ring Manager and Import a key

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **OpenPGP Security** tab.
4. In the OpenPGP Settings area, select **Launch OpenPGP Key Ring**.
5. Select **Import** to begin the key import process.



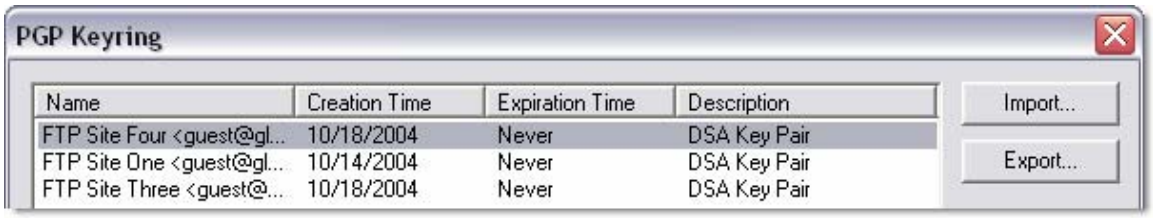
6. Select the file containing the key to be imported and select **Open.** The **Import OpenPGP Key** window closes and the imported file is now included in the Key Ring list.



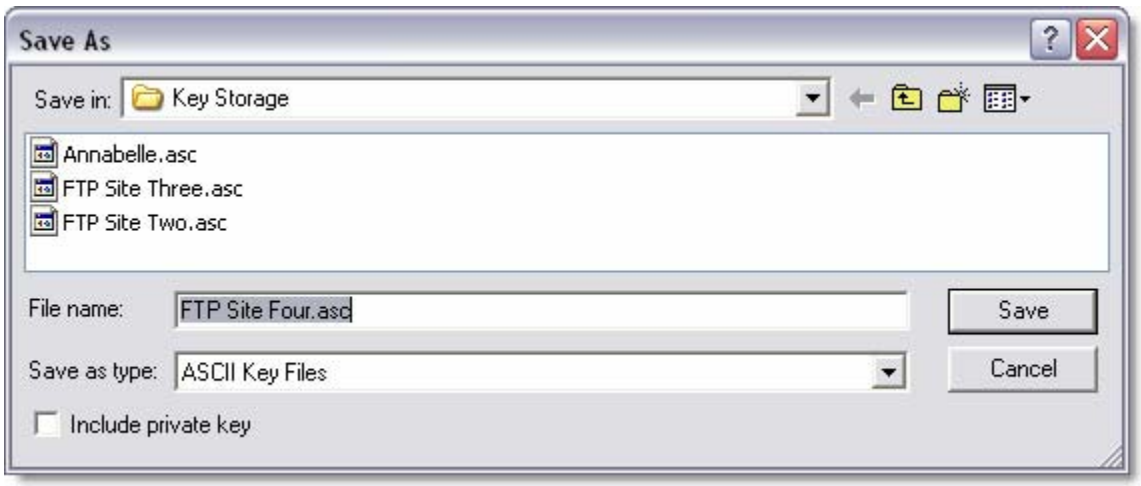
To access the Key Ring Manager and Export a key

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **OpenPGP Security** tab.
4. In the **OpenPGP Settings** area, select **Launch OpenPGP Key Ring**.
5. Highlight the file to be exported.

6. Select **Export** to begin the export process.



7. The **Save As** dialog appears. Select the folder you want to keep the new key file in.



Note:
Place a check in the box to include the private key in the export.

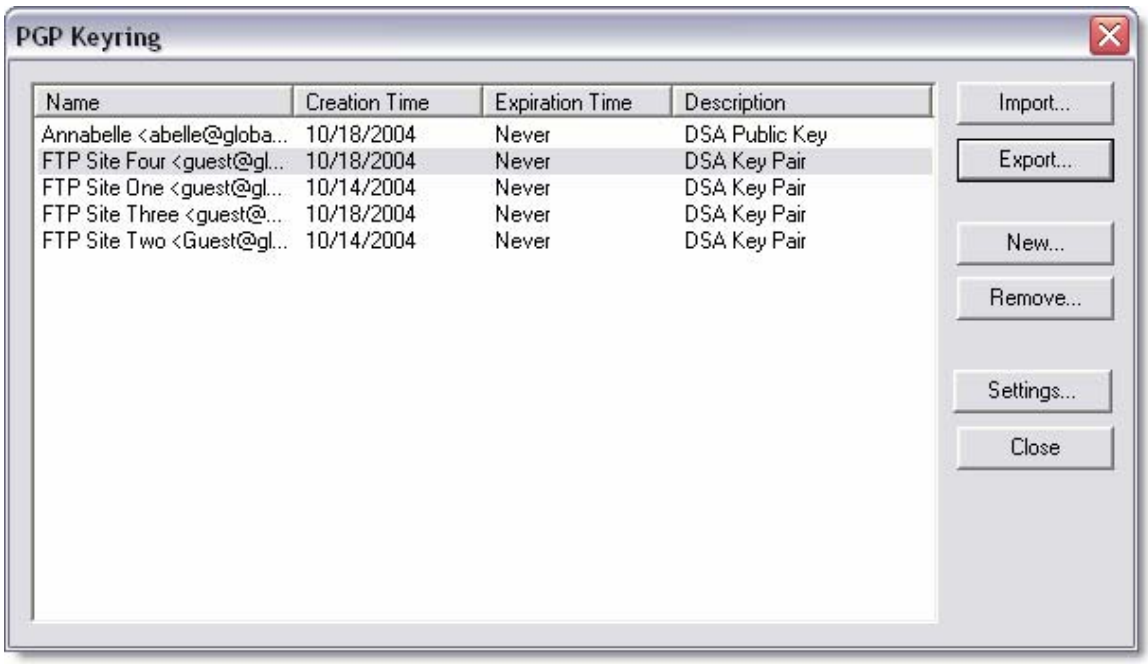
8. Select **Save** to export the file.

OpenPGP key ring manager

Use the OpenPGP key ring manager to create, delete, import, and export OpenPGP key pairs. You can also change or specify **key pair path settings**.

To access the Key Ring Manager

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **OpenPGP Security** tab.
4. Select **Launch OpenPGP Key Ring**.



Key pair path settings

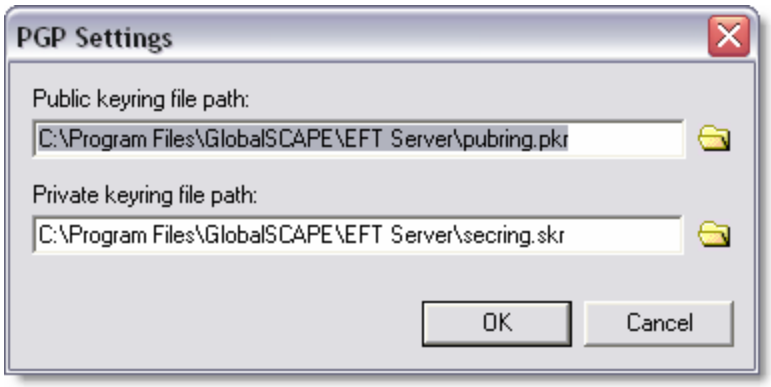
The default **Key Pair Path** settings can be viewed in the **OpenPGP Settings** window.

To access the OpenPGP Settings and change Key Path Settings

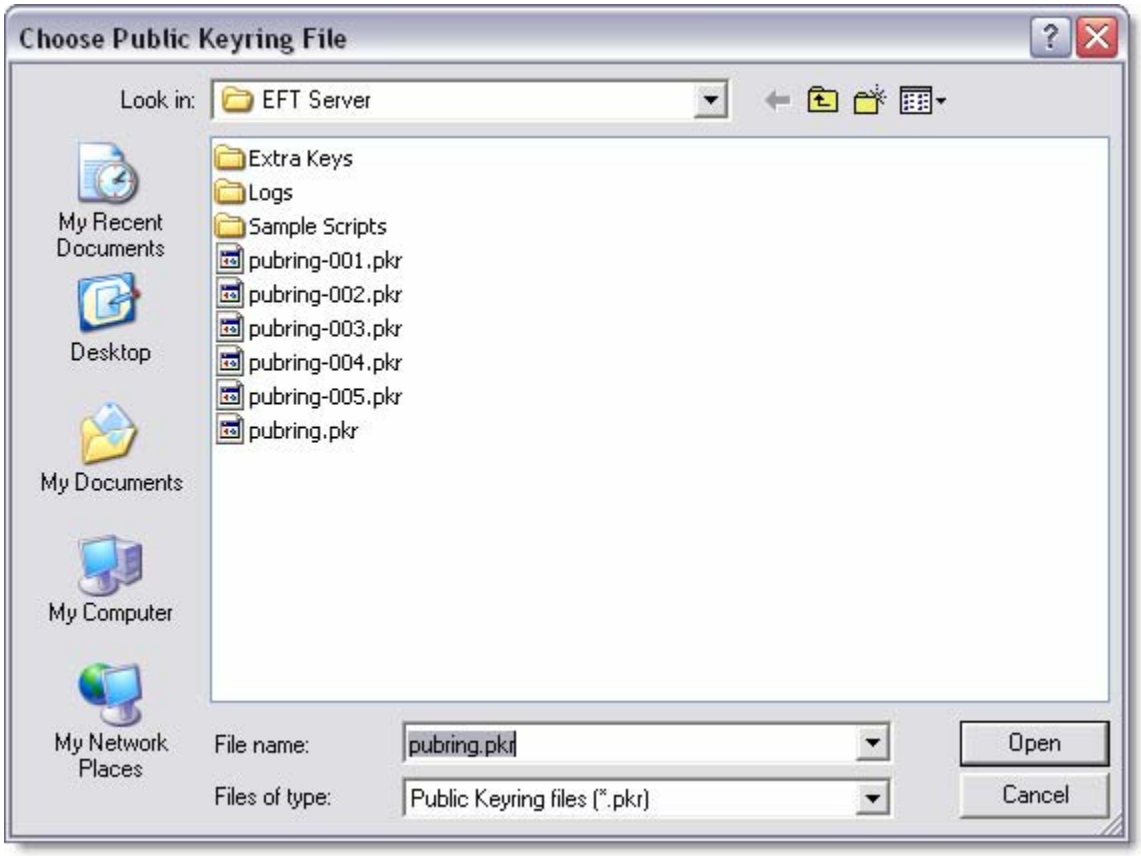
1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **OpenPGP Security** tab.
4. In the **OpenPGP Settings** area select the **Launch OpenPGP Key Ring** button.

To change Key Path settings

1. Select **Settings** in the **OpenPGP Key Ring** manager.



2. Select the folder icon to the right of the key path text box.



3. Highlight the key ring file to be changed.
4. Select **Open** to change the file path.

> **Note:**
> When key paths are changed the key list is automatically refreshed.

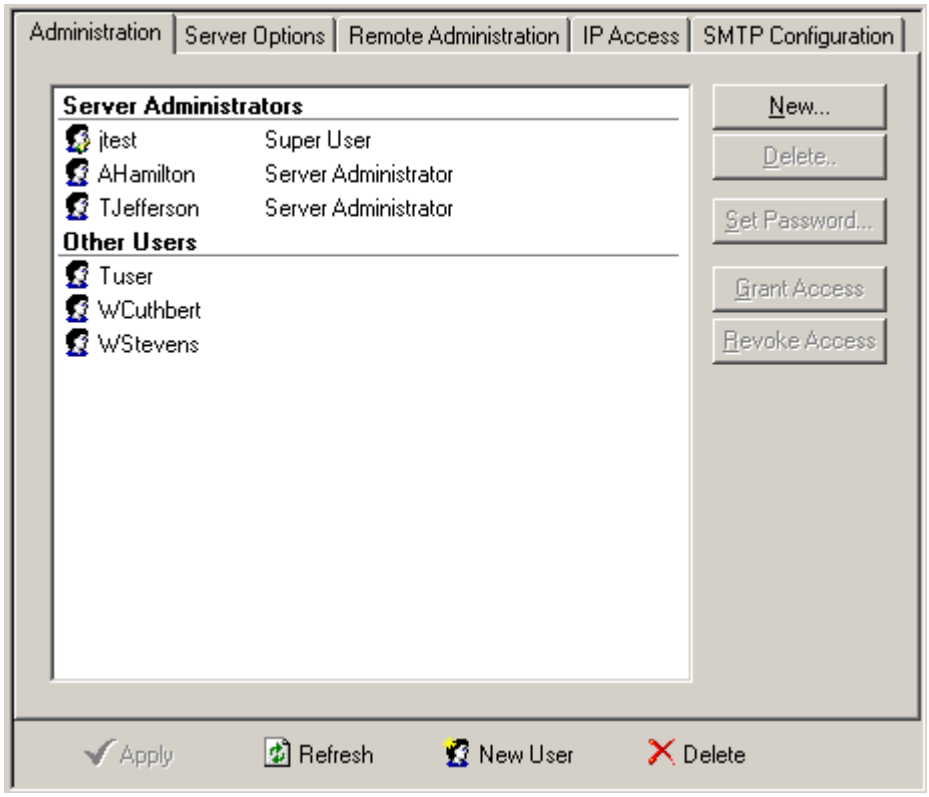
5. Select **OK** to close the OpenPGP Settings dialog.

Adding Site Administrators

You can give other people access to the administrative functions of Enhanced File Transfer Server by creating an administration account for them in the EFT Administrator. You can add accounts, grant and revoke access at the server and the site level.

To create a site administration account

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to add an administrative account to from the left-hand navigation tree.
3. In the right pane, select the **Administration** tab.



4. Select **New...** and add a user name and password for the new administrator account.

> **Note:**
> Passwords are case-sensitive.

5. If you want the new account to have site administration rights, select **Allow site administration**. This gives the new account administration access to the selected site.
6. Select **OK**. The new account appears in the Administration list.
7. You can grant (or revoke) access to any user (except the Super User) by selecting the user and select **Grant Access** (or **Revoke Access**).

Note:
You can also select and drag a user from one list to another.

Note:
To set or create Server administrative accounts, see Adding server administrators.

7

Users and User Setting Levels

How user setting levels work

Every client account or user must be a member of a User Setting Level. User Setting Levels exist within a Site. User Setting Levels consist of a group of settings used as a template. Each new user is assigned to a User Setting Level where settings determine how server resources may be used. One Setting Level may be quite restrictive, while another may allow more access to resources. Power users would be assigned to a setting level allowing greater flexibility in using server resources while guest users would be assigned to a more restrictive level where use of server resources is very limited. User Setting Levels allow an administrator to make changes at the User Setting Level that affect all users within the level. The basic profile of individual users can also be changed (overriding the template). Users can also be moved between User Setting Levels with a simple drag-and-drop. Users that are moved inherit the properties of the new User Setting Level, but retain any modifications (overrides) made by the administrator.

The server ships with one User Setting Level named **Default Settings**. Additional User Setting Levels can be added to define access to server resources for various types of users.

> **Note**:
> User Setting levels apply to server resources. Permissions assigned for **Groups** control access to folders on your system.

To create new user setting levels

1. At the bottom of the left pane, select the **Server** tab.
2. Expand a Server Group, Server, and Site.
3. Select **User Setting Levels.**
4. Select **New**.

Inheritance

All Users settings initially share those of the User Setting Level where the account was created. When you view user properties, inherited settings are marked by gray check boxes.

You can change a User's Setting Level by dragging and dropping them into a different level. The User's inherited settings change to reflect the settings of its new User Setting Level.

Overriding a user's inherited settings

You can override a User's inherited settings. The check boxes toggle through three settings:

- **Inheirited:** A gray check box means no changes have been made by the administrator to the settings inherited from the User Setting level. This is a neutral indicator and simply means User Settings for that parameter are unchanged for that particular user.
- **Overridden, Enabled:** A black check box means the administrator has overridden this inherited setting. This setting is *enabled* for the user even though it was disabled in the User Setting Level for this example.
- **Overridden, Disabled:** A blank check box means the administrator has overridden this inherited option. This setting is *disabled* for the User, even though it is enabled in the User Setting Level.

> **Note:**
> If a User account contains modified (overridden) settings and is moved to a new User Setting level, those modifications remain in effect at the new User Setting Level.

Creating user setting levels

You can create one or more user setting levels before or after creating users and subsequently assign users to the desired user setting level. This allows you to control the server's resources while still giving your users the flexibility they need to transfer essential files.

To create a new User Setting Level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select **Configuration > Create New User Setting Level** from the menu. The **Create New User Setting Level** dialog appears.
3. Select a Site from the pull down menu.
4. Enter a name for the User Setting Level.
5. Optionally, enter a description for the user setting level.
6. Select **OK**. The new user setting level displays.
7. Enter desired options in the **Main** tab. See Disabling Users and User Setting levels and Specifying a user's home folder for more information.
8. Change the **Login message** by entering or changing text in the text box.
9. Select the appropriate action from the drop-down menu above the text box.
10. Select **Apply** to make the change.
11. Select the **Security** tab. For more information, see:
    - Security Options
        - Disconnecting problem users
        - Allowing users to change their passwords
        - Allowing users to verify file integrity
        - Restricting User to a Single IP Address
    - Protocol permissions:
        - FTP
        - FTPS, SSL and TLS
        - SFTP
        - HTTP
        - HTTPS
12. Select the **Quota** tab. For more information, see:
    - Transfer Limits:
        - Setting maximum transfers per session
        - Setting maximum transfer size
    - Connection:
        - Enable Time Out

        - Set maximum transfer speeds
        - Setting maximum connections per IP
        - Setting maximum connections per User
    - Disks Quota:
        - Configure user disk quotas
13. Select **Apply** to make the changes.

Adding new users to a site

To add a new user to a site

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select **Configuration > Create New User** from the menu. The **New User Account Setup** dialog appears.
3. Select the Site you want to add a user to.
4. Enter the new user's **First Name** and **Last Name**. The server creates a **Username** in the format of [First_Initial_Last_Name]. You can optionally overwrite this.
5. Enter and confirm the **User Password**.
6. Select a **Password Type** from the pull down menu.
7. Optionally add a **Description**.
8. Select **Next**.
9. Make a selection from the **Place user in the following User Setting Level** pull down menu.
10. Select both **Create user home folder** and **Grant FULL permissions...** to create a user folder located in the site root folder and to give the user full permissions to that folder.
11. Select **Next.**
12. In the **Not a member of** pane of the **Setup user groups** section, select one or more Groups where you want the new User to be a member. By default, all new Users are members of the **All Users** group.
13. Select **Finish** to generate the new user.

User and User Setting Level Settings

Disabling users and user setting levels

To disable an user setting level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.

2. Select the User Setting Level you want to disable from the left-hand navigation tree.
3. In the right pane, select the **Main** tab.
4. Clear **Enable this settings level**.
5. Select **Apply**. A red "X" appears in the right-hand navigation pane over the User Setting Level and any users that have not been enabled independently of the setting level.

To disable a user

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User you want to disable from the left-hand navigation tree.
3. In the right pane, select the **Main** tab.
4. Clear **Enable this user account**.
5. Select **Apply**. A red "X" appears over the user icon in the right-hand navigation pane.

To disable a user on a specific date (account expiration)

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User you want to set an expiration date for from the left-hand navigation tree.
3. In the right pane, select the **Main** tab.
4. Select **Expire this account after** and fill in the expiration date. Select the pull down menu to select a date from the pop-up calendar.
5. Select **Apply**. The User account is disabled on the specified date.

Enabling SSL at the user and user access level

Enhanced File Transfer Server has robust SSL configurations that allow you to configure SSL connections on all sites, at the site level, at the user setting level, or at the user level. You can also configure SSL with a combination of these four levels.

> **Note:**
> In order for SSL support to be available at any other level it must first be configured at the Site level.

To enable SSL at the user setting level

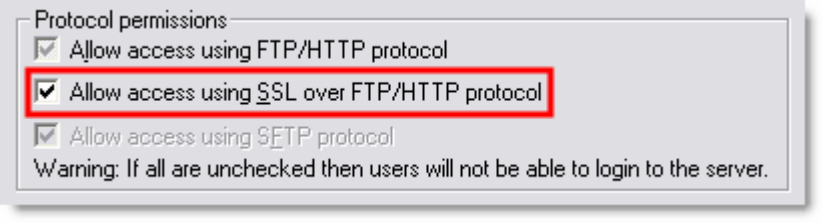
1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.

4. Select **Allow access using SSL over FTP protocol** to allow users in the access level to connect using SSL.
5. Either:
    - Clear **Allow access using FTP protocol** to allow only SSL connections, OR
    - Select **Allow access using FTP protocol** to allow both standard FTP and SSL connections.

To enable SSL at the user level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.
4. Toggle the **Allow access using SSL over FTP protocol** check box until it's a black check in a white box to allow users to connect to the server using SSL.
5. Either:
    - Clear **Allow access using FTP protocol** to allow only SSL connections, OR
    - Select **Allow access using FTP protocol** to allow both standard FTP and SSL connections.

Note:
Gray check boxes indicate that the user is inheriting that option from the user setting level it belongs to. See Inheritance for more information.



Enabling HTTP access

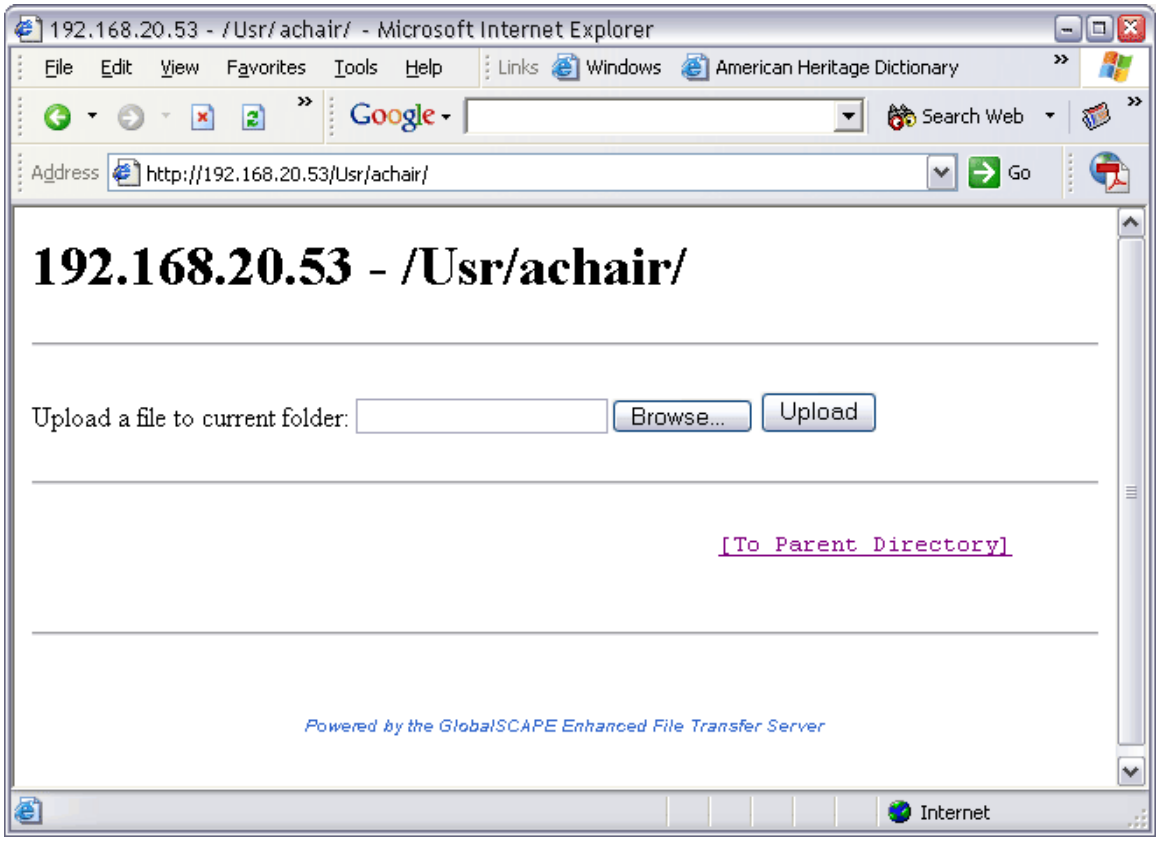
To enable HTTP transfers at the user and user setting levels

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user or user setting level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.
4. Under Protocol permissions, select **Allow access using HTTP Protocol**.
5. Select **Apply** to save and implement the changes.

Note:
HTTP transfers must be enabled at the site level to allow users HTTP access.

HTTP form upload

When HTTP transfers are enabled and a user has permissions to upload using HTTP, a form appears at the top of the user's browser when they navigate to their user directory that allows them to upload files to the EFT Server. Users can enter a direct path (UNC is supported if the OS the user is using also supports it) or they can select **Browse...** and locate the file with the browser's standard file dialog. Note that this upload form limits the user to uploading one file at a time.



EFT Upload Form

Restricting a user to a single IP address

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user setting level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.
4. Select the **Restrict to this IP** check box and enter the IP address. Wildcards or ranges are not accepted.
5. Select **Apply.**

Specifying a user's home folder

You can determine the user's login folder at the user and User Setting Level. This is typically set at the user level.

To set a user's home folder

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Main** tab.
4. Select **Home Dir**.
5. Select the browse button next to the **Home Dir** box.
6. Select the folder you want the user to be placed in when they log on.
7. **Select Apply**.

Note:
Selecting **Treat home folder as default root folder** makes the home folder *the users* root folder.

To verify that the User Setting Level is not controlling the user's home folder

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User Setting Level of the user you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Main** tab.
4. Clear **Home Dir**. Note that selecting this box forces the default root folder of all users in the setting level to a specified folder.
5. Select **Apply**.

Changing a user's password

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user you want to configure from the left-hand navigation tree.

3. In the right pane, select the **Main** tab.
4. Select **Change Password**. The Change User Password dialog appears.
5. Enter and confirm the password.
6. Choose the **Password Type** from the drop down list. You may choose:
    - **Standard** – A plain text password is required.
    - **Anonymous** – Any password, including nothing, allows an anonymous connection.
    - **Anonymous (Force Email)** – Any well formed email address is the password
7. Select **OK**. The Change User Password dialog closes.
8. Select **Apply**.

Configuring user details

User details are the account specific details associated with the particular User, such as phone number, pager, and email address. Some of these fields (such as the email address) can be used in other parts of the program (such as the Event Rules) to notify the user of a completed transaction.

To configure User details

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Details** tab.
4. Fill out all necessary fields.
5. Select **Apply**.

Accelerating transfers with Mode Z

Mode Z compression compresses files on the fly for file transfers, saving bandwidth and improving transfer times. The client must support MODE Z also to take advantage of this feature. If MODE Z is enabled, Secure FTP Server will listen for MODE Z requests, then enable it for subsequent transfers from the client that requested it.

To allow a client to use Mode Z compression

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user or user setting level you want to configure from the left-hand navigation tree.
3. Select the **Security** tab.
4. Select Allow **MODE Z Compression**.

Allowing users to change their passwords

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.
4. Select the **Allow PSWD command for client change password request** check box.
5. Select **Apply**.

To prohibit users from changing their passwords

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user or Using Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.
4. Clear **User can change password (SITE PSWD command)**.
5. Select **Apply**.

Allowing users to verify file integrity

Although TCP/IP checks that all packets are received, malformed packets or other mishaps can occur, leading the FTP client to believe that a transfer was successful when it was not.

Enhanced File Transfer Server's file integrity command is defined as XCRC. Once an XCRC enabled client performs a transfer, it can request the server to do a checksum calculation on the file. If it matches the checksum on the client, then the transfer is deemed successful. Performing XCRC checksum calculations are processor intensive so enable or disable the feature accordingly.

To enable file integrity (XCRC) checking

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Security** tab.
4. Select **Allow XCRC command** to enable XCRC file integrity checking.
5. Select **Apply**.

XCRC

XCRC is a proprietary command and is not defined nor endorsed by any FTP related RFC. Competing servers who wish to implement this command may do so using the following syntax: described below.

```
XCRC <File Name>
XCRC <File Name>, <EP>
XCRC <File Name>, <SP>, <EP>
```

SP = Starting Point in bytes (from where to start CRC calculating)
EP = Ending Point in bytes (where to stop CRC calculating)

FTP client log example

Client command:

```
COMMAND:>      XCRC "/Program Files/MSN Gaming
Zone/Windows/chkrzm.exe" 0 42575
```

- SP and EP are optional parameters. If not specified then it calculates the CRC for the whole file. If only EP is specified, then the CRC calculation starts from the beginning of the file to the EP.
- This command can be used for a single file at a time. It does not allow file lists as parameters.
- The standard CRC32 algorithm is used (for speed and efficiency).
- A client can invoke this command for uploads, downloads, single and Multi-Part transfers.

Server replies:

```
250 <XCRC>.
```

This returns the calculated CRC value.

```
450 Requested file action not taken.
```

This indicates that the file is busy.

```
550 Requested action not taken.
```

This indicates that the file is not found, has no read permission, or the SP or EP are not correct.

Setting maximum transfers per session

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Quota** tab.
4. Select the **Uploads or Downloads per session** check box and enter a number. This number will be the maximum allowed during the user's session.
5. Select **Apply**.

Setting maximum transfer size

The maximum transfer size limits the user to a specified number of uploaded or download kilobytes per session. File Transfer Protocol does not send information to the server regarding the number of bytes that a user sends.

A user can start a transfer of virtually any size; however, once the limit is reached, the server will not transfer the rest of the file.

To set the maximum upload size

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Quota** tab.
4. Select **Max Upload/Download Size** and enter the maximum amount of data (in kilobytes) the user may transfer during a session.
5. Select **Apply**.

Setting maximum connections per IP

You can set the maximum number of simultaneous connections emanating from a same IP address at three levels:

- The Site level
- The User Setting Level
- The User level

Note:
The Site level sets the limits of the User and User Setting Levels.

To set maximum connections from same IP at the site level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Advanced** tab.
4. Select **Max connections from same IP** and enter a number. If the box is clear a user can create as many concurrent connections to the site from the same IP address that are allowed by the limits defined at the User or User Settings level.
5. Select **Apply**.

To set maximum connections per user account at the user and User Setting level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.

2. Select the user or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Quota** tab.
4. Select **Max connections from same IP** and enter the maximum times you wish that **User** account or users in that **User Setting level** to be able to simultaneously connect to the site from the same IP address. Note that a gray check on a **User** account indicates the account is inheriting parameters from the **User Setting or Site level**.
5. Select **Apply**.

Setting maximum connections per user

The maximum number of simultaneous connections for a User are set at three levels:

- The Site level
- The User Setting Level
- The User level

Note:
The Site level sets the limits of the User and User Setting Levels. For example, if the Site level **Max connections per user** is set to five, and a user's User level **Max connections per user** is set to ten, the user can have a maximum of five simultaneous connections.

To set maximum connections per user at the site level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Advanced** tab.
4. Select the **Max connections per user** check box and enter a number. If the box is clear a user can create an unlimited number of concurrent connections to the site (or according to the limits defined at the User or User Settings level).
5. Select **Apply**.

To set maximum connections per user account at the user and User Setting Level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Quota** tab.
4. Select the **Max connections per user** check box and enter the maximum times you wish that **User** account or users in that **User Setting Level** to be able to simultaneously connect to the site. Keep in mind that a gray check on a **User**

account indicates the account is inheriting parameters from the **User Setting or Site level**.

5. Select **Apply**.

Setting time-out

Setting a timeout value causes the server to disconnect a user after inactivity for the specified number of seconds.

To set Time Out function at the User and User Setting Level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the user or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Quota** tab.
4. Select **Enable Time Out (sec)** and enter the number of seconds you wish to limit that **User** account or users in that **User Setting Level** to be inactive. Keep in mind that a gray check on a **User** account indicates the account is inheriting parameters from the **User Setting or Site level**.
5. Select **Apply**.

Note:
Many popular FTP clients have keep-alive functionality that will attempt to issue do-nothing commands such as NOOP in order to simulate user activity and prevent a time-out. If **Block anti-timeout schemes** is enabled for the server, such do-nothing commands are ignored and will not reset the counter for the time-out limit.

Setting maximum transfer speeds

You can control a user's maximum transfer speeds at three levels:

- The site level
- The user setting level
- The user level

Note:
The Site level sets the limits of the User and User Setting Levels.

To configure maximum transfer speeds at the Site level

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Advanced** tab.

4. Select the **Max transfer speed (KB/s)** check box and enter the maximum transfer speed for the site. The server does not set a maximum transfer speed if the box is cleared.
5. Select **Apply**.

To configure maximum transfer speeds at the User and User Setting levels

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User or User Setting Level you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Quota** tab.
4. Select the **Max transfer speed** check box and enter the maximum transfer speed (in Kilobytes per second) for the user.
5. Select **Apply**.

Configuring user disk quotas

Disk space management is an important aspect of server administration. Setting quotas allows you to specify the maximum amount of disk space available to each user in their home folder.

Max disk space sets the maximum disk space that users can consume in their home folders. The server administrator can assign each user a **Max disk space** for that user's home folder. As the user uploads and downloads, the server measures the user's **Used disk space**. Uploading files increases the **Used disk space** and deleting files decreases this number. If a user uploads too many files and the **Used disk space** equals the **Max disk space** that the server administrator assigned, the user has to delete files before uploading again.

When a server administrator uses Windows Explorer to add or delete files, the server will update file quotas appropriately. This means that a user's **Used disk space** will change when the administrator adds or deletes files in the user's home folder. Additions and deletions to a user's folder that are performed outside of server will only be monitored by the server and not prohibited, even when the number of files added exceeds the **Max disk space** allowed. In this situation, the user's file quota would be updated and the user would be prohibited from uploading until the **Used disk space** was less than the **Max disk space**.

To set a user's disk quota

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User Setting level or user you want to configure from the left-hand navigation tree.
3. In the right pane, select the **Quota** tab.

4. Select **Enable disk quota for user's home folder** and enter the maximum number of kilobytes the user may use in their home folder.
5. Select **Apply**.

Multi-part transfers

Enhanced File Transfer Server supports multi-part transfers from advanced FTP clients such as CuteFTP Professional. The user must have appropriate privileges and be authorized to connect multiple times concurrently. The connecting client takes care of most details, including splitting the file apart, sending the multiple parts, and then requesting that the server to join them again upon receipt. The COMB command joins the parts back together. The benefits of segmented (multi-part) and concurrent delivery for accelerated transfers include:

- Accelerate throughput and maximize available bandwidth available to the client by allowing uploaded files to be split apart and transferred in multiple segments simultaneously.
- Command can be toggled on or off.

The COMB command is a proprietary command and is not defined nor endorsed by any FTP related RFC. However, the command can be integrated with other servers using the following syntax:

```
COMB <TF> <SF 1> … <SF n>
```

where

```
<TF>  is the path to target file, which will contain the
combined data from the source parts.
<SF #> are the source files (parts).
```

Combine ***n*** source files (SF 1...***n***) into one file (TF).

- If the target file already exists, then server appends source files to it.
- The server will delete all the source files once combined successfully.
- All file names should be in quotes.

8

Permission Groups

Permission groups

Permission Groups set user access permissions to folders. Permission **Groups** are different from **user setting levels and users**. User setting levels control access to server resources such as bandwidth allowances and connectivity privileges.

Enhanced File Transfer Server creates three default permission groups for every site: Administrative, All Users, and Guests.

You can configure permission groups of your own or modify the settings for the default groups. Consider your security and access needs, then configure permission groups according to those needs. Add users to groups accordingly.

To view permission groups

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Expand a Server Group, Server, Site and **Groups**.

To add users to a permission group

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-
3. Expand a Server Group, Server, Site and **Groups**.
4. Select a permission Group.
5. In the right panel, click a User in the **Not a member of** window and click the left arrow. Users can be members of more than one Group at a time.

Note:
If a User is a member of more than one Group and you have not modified that User's permissions, that User will have the highest level of access allowed to any folder or folder action. As the administrator, you can individually modify User permissions. The modified permissions outweigh all Group permissions. For instance, a User is a member of three Groups that all have upload permissions to a particular folder, but you have denied that specific User permission to upload to the folder, then the User will be unable to upload to the folder.

Creating groups

You can create a permission group and add any users from the site to a group. You can then grant permission to folders by groups rather than granting permissions to each individual user.

To create a permission group

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Group you want to configure from the left-hand navigation tree.
3. Select **New** on the right-hand pane.
4. Select a site from the **Site** drop down list.
5. Enter a name for the Group in the **Group Name** box.
6. Select **OK**. The new group appears under the site selected in **Groups**.

Deleting groups

Deleting permission groups does not delete individual users.

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Group you want to configure from the left-hand navigation tree.
3. Right-click and choose **Delete** or select **Delete** from the toolbar.
4. Select **Yes** when asked **Remove group "[groupname]"?**

Adding or removing users

You can add any user on a site to any group on the same site. You cannot add users from one site to another site.

To move users into a group

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Group you want to configure from the left-hand navigation tree.

3. Select a User and use the arrows in the right panel to move the User to the desired membership.
4. Select **Apply**.

To move users out of a group

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Group you want to configure from the left-hand navigation tree.
3. Select a User and use the arrows in the right panel to remove the User to the desired membership.
4. Select **Apply**.

9

Virtual File System Permissions

Virtual File System (VFS)

The VFS lets you grant access to files and folders on your system. After selecting the left window's **VFS** tab, you can choose which files and folders will be available to users and then configure Group and User permissions for these folders.

Types of folders

The Virtual File System (VFS) allows you to create physical folders and virtual folders.

- **Physical folders** are folders you create on your hard drive from the server. They are simply called folders within the program.
- **Virtual folders** reference, or point to, currently existing folders on your computer or another system. Because a virtual folder name is only an alias for the real folder, when you create a virtual folder you do not have to give it the same name as the actual folder it references.

Permissions

You make the files, physical folders, and virtual folders available to users by granting permissions. To view the folders currently on the server, create new folders, or delete existing folders, select the **VFS** tab at the bottom of the left window.

VFS Permissions are constructed to allow users the least restrictive access to folders. For example, a user is a member of one group that has read, upload, download and delete permissions to a folder. Even if the user is a member of another group that has only download permissions to the same folder, the user will be able to read, upload, download and delete files from that folder.

VFS rules for folder access

The VFS access system is regulated by three rules. The rules differ from the rules that govern Windows NT permissions.

1. **User permissions are given priority.**

   If the server finds user specific permissions that are not those from groups in the folder that the user wants to access the server does not look for any group

permissions. The server gives priority to individually configured permissions. For example, there is an individual user with the user name Bob. Bob is a member of two permission groups that have download and list permissions only for Folder1. However, you have decided that you want to give Bob full permissions for Folder1 without creating a new permission group, so you add Bob to the file and give him full permissions. Since the server looks for these individual user permissions first, then Bob will have full permissions for Folder1 no matter how his group membership is configured. This same rule also implies that if Bob has individual permissions that only allow him to download files from that particular folder, it does not matter if he is a member of two groups that have full permissions for the folder. Bob will only have permission to download files.

2. **If a user does not have individual permissions for a folder and is a member of more than one group, the server gives the user the least restrictive access for the folder.**

   From their groups, users receive all the permissions available for the folder. For example, suppose a user with the user name Jan is a member of two groups, Group1 and Group2, that both have permissions for a particular folder, Folder2. If Group1 has download permission and Group2 has upload permission then Jan will have both upload and download permissions for Folder2.

3. **The All Users group is the same as any other group except that it can't be removed from the root folder permissions list.**

   You can use the All Users group to determine inherited permissions from the parent folder in the EFT Administrator. If you change any inherited permissions for the All Users group, the server display a screen to make sure you want to change the inherited permissions.

VFS permission inheritance

Any time a new folder is created it inherits permissions from its parent folder. Using permission inheritance, administrators can make global access changes by simply changing group access in a parent folder.

You can modify a folder's permissions even while it is inheriting permissions from a parent folder.

To modify a permission

1. Select a folder in the VFS structure.
2. Highlight an existing group or user or click **Add...** to add a User or Group to the selected folder.
3. Select the user or group you wish to modify permissions for.
4. Leave **Inherit permissions from parent folder** selected and then select any other additional permissions.

Note:
This will affect all sub-folders containing this User or Group who have the option **Inherit permissions from parent folder** turned on.

Disabling inheritance

In the course of server administration, you may want to reconfigure a folder's settings. You can override a user's inherited settings by clearing the **Inherit permissions from parent folder** check box.

If you manually clear **Inherit permissions from parent folder,** you can configure the folder's permissions the way you want them. If you later decide you want the folder to inherit permissions again, simply select I**nherit permissions from parent folder**.

The following instructions show you how to prevent a folder from inheriting its parent folder's permissions, force a single modified folder to begin inheriting permissions to sub-folders or reset all subfolders of a particular parent folder to inherit permissions from that parent.

To stop a folder from inheriting permissions

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.
2. Select the folder you want to configure from the left-hand navigation tree.
3. In the right pane, clear **Inherit permissions from parent folder**.
4. Select from the following options:
   - **Copy** copies the permissions from the parent. You may later edit the permissions.
   - **Remove** removes all inherited permissions.
   - **Cancel** cancels the change.

To force a folder to inherit permissions from a parent folder

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.
2. Select the folder you want to configure from the left-hand navigation tree.
3. In the right pane, select **Inherit permissions from parent folder**.
4. Select from the following options:
   - **Copy** copies the permissions from the parent. You may later edit the permissions.
   - **Remove** removes all inherited permissions.
   - **Cancel** cancels the change.

To reset folder permissions for all subfolders of a parent folder

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.

2. Select the top level folder from the left-hand navigation tree.
3. Right-click the folder and select **Reset Subfolders.**

Note:
This deletes all existing permissions from the subfolders and forces them to inherit permissions from the selected folder.

Creating a new physical folder

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.
2. From the left-hand navigation tree, right-click the folder you want ro create a subfolder in.
3. Choose **New Physical Folder...** from the menu.
4. Type a name for the new folder, and select **OK**.

Changing the name of a physical folder

You can change the name of a physical folder on the server but you cannot change the name of a virtual folder.

To rename a physical folder

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.
2. Select the folder you want to configure from the left-hand navigation tree.
3. Choose **Rename Folder**.
4. Type the new name and press ENTER.

Deleting a physical folder

When you delete a physical folder from within the server, the folder is deleted from the EFT server and your computer's hard drive.

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.
2. Select the folder you want to delete from the left-hand navigation tree.
3. Choose **Delete Folder** from the menu.
4. Select **Yes** when asked **Are you sure you want to remove the folder "[foldername]"?**

Creating a new virtual folder

Virtual folders reference currently existing folders on your computer's hard drive. A virtual folder name is only an alias for the real folder. When you create a virtual folder you do not have to give it the same name as the actual folder it references.

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.

2. Select where you want to add a virtual subfolder from the left-hand navigation tree.
3. Choose **New Virtual Folder...** from the menu.
4. Type a name for the folder in the **Alias** box.
5. Choose the target folder by typing the path in the **Target** box, or click the little yellow folder and browse to the target folder.
6. Select **OK**.

Deleting a virtual folder

When you delete a virtual folder, you merely delete a pointer, not the actual folder it references.

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.
2. Select the folder you want to delete from the left-hand navigation tree.
3. Choose **Delete Folder** from the menu.
4. Select **Yes** when asked **Are you sure you want to remove the folder "[foldername]"?**

Setting folder permissions

You set permissions for physical and virtual folders the same way.

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.
2. Select the folder you want to configure from the left-hand navigation tree.
3. Select the user or group you want to modify or click **Add...** to add a User or Group.
4. Select or clear the appropriate permission check boxes in the **File**, **Folder**, and **Contents** groups.
5. Select **Apply**.

Resetting folder permissions

Resetting folder permissions from a **parent folder** forces subfolders to exactly mirror those permissions. This simplifies the permissions status of these folders, making them more predictable

To reset folder permissions from a parent folder

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.
2. Select the parent folder you want to configure from the left-hand navigation tree.
3. Right-click the folder and choose **Reset Subfolders**.
4. Select **OK**.

Note:
Resetting folder permissions from a parent folder differs from manually changing the inheritance values of subfolders because in a subfolder you have the option to either mirror the parent folder's permissions or to keep permissions for any new Users and Groups you have added while also mirroring the permissions for all Groups in the parent folder.

Mapping a virtual folder to a network drive

Factors to consider before mapping a folder to a network drive

If you want to map a virtual folder to a network drive:

- Are you the administrator of the computer where you are running the service? If not, you need to become the administrator of this computer, or have your system administrator make the changes.
- Are you in a domain or a workgroup?
- Do you understand how to use UNC path names? When you are remotely administering the server, you will need to enter UNC path names.

Necessary user accounts

In order to map to a network drive, establish the following server user accounts:

1. A separate account for the GlobalSCAPE EFT Server service. It must have full access to any folder you want to make available on the server.
2. A **EFT Server** administrator account. Your account on the computer where the server is running must have full access to any folder you want to make available on the server.

To map to a network drive in a domain

1. Through the Windows **Services** control panel, create and assign an NT account on the computer where the service is installed.

   Note:
   This should not be the default (system) account.

2. Assign restrictive file and folder permissions for this account.
3. In EFT Administrator, create a virtual folder for a folder on your networked drive. If you are remotely administering, or the drive is not mapped to your computer, make sure that you use a UNC path name
4. Assign permissions for users by selecting the **VFS** tab within server, selecting the folder in question and then selecting or clearing the appropriate permission boxes.

Note:
You need to have administrative rights on the system the service is running on in order to create accounts.

To map to a network drive in a workgroup

1. Through the Windows **Services** control panel, create and assign an NT account on the computer where the GlobalSCAPE EFT Server service is installed.

Note:
This should not be the default (system) account.

2. Assign restrictive file and folder permissions for this account.
3. Create a matching account on the target remote machine. Make certain it uses the SAME user name and password. Restrict permissions to this account to allow users access to only those folders they need.
4. In EFT Administrator, create a virtual folder for a folder on your networked drive. If you are remotely administering, or the drive is not mapped to your computer, make sure that you use a UNC path name.
5. Assign permissions for users by selecting the VFS tab, selecting the folder in question and then selecting or clearing the appropriate permission boxes.

Note:
You must have administrative rights on the system the service is running on in order to create accounts.

Streaming repository encryption

Files stored on the disk in EFT's Virtual File System can be transparently encrypted during read/write. Data is encrypted as it is written to disk, and decrypted prior to transmission.

To enable streaming repository encryption

1. In EFT Administrator, select the **VFS** tab. You should be connected to the server.
2. Select the parent folder you want to configure from the left-hand navigation tree.
3. Right-click the folder and choose **Encrypt Contents**.
4. Select **OK**.

Note:
If you turn on this feature, it's a good idea to set up an appropriate back up measures to protect your data. If you need to recover a private key to decrypt data, and that key is lost, you will not be able to recover the data the key protects. Streaming repository encryption leverages Microsoft's

EFS. If you need more information on setting up appropriate back up procedures, see Best Practices for the Encrypting File System.

Note:
Streaming repository encryption is not available for systems running on FAT32 filesystems. NTFS is required.

Note:
Streaming repository encryption is not available with NT authentication due to limitations of NT authentication. If you require this feature with an NT set up, LDAP authentication is recommended.

10

Authentication

Authentication types

Enhanced File Transfer Server supports three database types for authenticating users: Enhanced File Transfer Server, NT Authentication, ODBC, and LDAP Authentication. Once a site has been configured through the **Create Site Wizard**, you cannot change the authentication method.

- **GlobalSCAPE EFT Server Authentication** does not rely on outside sources for user information (accounts protected from the OS). All information is contained within the .aud file located in the server engine (cftpste.exe) folder. All information is encrypted and can only be modified through the EFT Administrator.
- **ODBC Authentication** allows all users in an external ODBC database to have access to the server. See the topics under ODBC book for more information on configuring ODBC authentication.
- **NT (NTLM/AD) Authentication** Using this method, Enhanced File Transfer Server assigns permissions to users from the NT User Database on the system that is running the server. Enhanced File Transfer Server queries the Primary Domain Controller (PDC) for your domain and adds all domain users.
- LDAP

ODBC

Using an ODBC data source for user authentication

Enhanced File Transfer Server allows you to use any ODBC compatible database as a source for user authentication. You may add and remove users and set certain permissions using your existing database utility or through the EFT Administrator.

In order to use an external ODBC data source you must:

- Create tables in an ODBC data source.
- Establish a System Data Source Name (DSN) in the ODBC Source administration tool.
- Set GlobalSCAPE EFT Server to use the System DSN.

- Have Microsoft Data Access Components (MDAC) 2.6 or higher installed.

If you are using the server on Windows XP, you do not need to install MDAC 2.6 or higher on your computer. For any other Windows operating system you can download **MDAC** 2.6 or 2.7 from http://www.microsoft.com/data/download.htm

If you are using an Access database, you may also need to download a Jet driver. For more information about Jet drivers, see http://support.microsoft.com/default.aspx?scid=kb;en-us;Q282010.

For more information, see http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q271908.

Creating tables for your ODBC data source

You must create two tables in the database for your data source:

The **ftpserver_users** table lists the user accounts and permissions groups in the site. A user account uses the information from all fields. A permissions group only uses the ID, Name, and Description fields and is used only for organizational purposes, not as a user login.

ftpserver_users: Table			
Field Name	Data Type	Field Size	Description
ID (Primary Key)	AutoNumber	Long Integer	User ID
Name	Text	50	Login name for this user
Password	Text	200	Password for this user
Description	Text	200	Description for this user
Type	Number	Integer	0=Group, 1=User
Password_Type	Number	Integer	Standard, OTP_MD4, OTP_MD5: Differentiates Regular vs. SKEY (OTP) password type. 0 = standard FTP password, 1=MD4 OTP, 2=MD5 OTP.
MD_Iter	Number	Long Integer	Current MDX iteration – used by OTP accounts only
OTP_Seed	Text	16	OTP Seed to be used for MDX Passwords – used by OTP accounts only.
Anonymous	Number	Long Integer	0=Normal Password, 1=Any password
Anonymous_Email	Number	Long Integer	0=Any anonymous password, 1=Email password required
Fullname	Text	200	User's full name
Email	Text	200	User's email address

Phone	Text	200	User's phone number
Pager	Text	200	User's pager number
Fax	Text	200	User's fax number
Comments	Text	200	User comments
Enabled	Number	Integer	0=Account disabled, 1=Account enabled

The **ftpserver_ids** organizes users into "groups" of permission levels. For each permissions group to which a user belongs there should be one entry in the table below.

ftpserver_ids: Table			
Field Name	Data Type	Field Size	Description
ID	AutoNumber	Long Integer	Unique ID for the record (key field).
User_ID	Number	Long Integer	This value refers to a user record in the ftpserver_users table. A corresponding (where ftpserver_ids.User_ID = ftpserver_users.ID) ftpserver_users record must exist with Type = 1.
Group_ID	Number	Long Integer	This value refers to the user setting level that the User_ID user record belongs to. A corresponding (where ftpserver_ids.Group_ID == ftpserver_users.ID) ftpserver_users record must exist with Type = 0.

Establishing a system data source name (DSN)

After you have created your database, you must associate it to your system.

To establish a system DSN

1. In Windows, open your **Control Panel**.
2. Select the **Data Sources (ODBC)** administrative tool.
3. Select the **System DSN** tab.
4. Select **Add**.
5. Select the appropriate driver from the list. There is a sample Microsoft Access (**GSFTPS.mdb**) database included within the installation folder.
6. Select **Finish**.
7. Enter the **Data Source Name** and **Description**. The default **DSN** is **GSFTP Server**.
8. Select **Select** and choose the database file you created when following the steps described in Create Tables for your ODBC data source or the supplied database described in Step five.
9. Select **OK**.

Using a DSN-less connection with ODBC authentication

You can create a Site with a DSN-less connection to your authentication database. If you have several simultaneous database connections, a DSN-less connection may be slightly faster than a DSN connection.

To create a site with a DSN-less connection

1. Open **EFT Serve**r.
2. In EFT Administrator, select **Configuration > Create New Site** from the menu.
3. Give the site a name, choose the IP address and Port.
4. In the **Authentication method** list, choose **ODBC Authentication**.
5. Click **Advanced**. The **Authentication Provider Options** window appears.
6. Enter the connection string in the box and click **OK**.
7. Click **Next** to continue with your site creation.

To create the string for a DSN-less connection

You must know the correct driver to use with your database. Create a connection string and enter it into Enhanced File Transfer Server. The connection string includes the name of the driver you need for your database, the location of your database, the name of your database, and, if necessary, a user name and password to access the database.

For local databases the connection string must include

- Provider [Provider=]
- Driver [DRIVER=]
- Database path and name, including the file extension [Dbq=]
- Username [Uid] and Password [Pwd] are required only if the database is password protected

For remote databases your connection string must include

- Driver [DRIVER=]
- Server [SERVER]
- Database [DATABASE]
- Username [UID]
- Password [PWD]

Examples

If you are pointing to Access 2000 database on the local machine named **Example** that was in the **xyz** sub-folder of your **c** drive the connection string is:

Provider=MSDASQL;Driver={Microsoft Access Driver(*.mdb)}Dbq=c:/xyz/Example.mdb;Uid=;Pwd=;

If you have a remote MYSQL database named **Example** your connection string is:

Provider=MSDASQL;DRIVER={MySQL ODBC 3.51 Driver};SERVER=10.10.10.1;DATABASE=Example;UID=myusername;PWD=mypassword;

Note:
Do not put any line breaks in your connection strings.
You must have MDAC version 2.7 or higher to use a DSN-less connection.

NT Permissions

NT permissions

After it is installed, Enhanced File Transfer Server has access to local folders and files. To run it as a service with permissions to the network and mapped drives; however, you must create an NT account for the server, assign the server service to the account, and log the server on as a service.

Setting permissions for EFT Server user accounts in Windows NT

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

Note:
Using NT Authentication, users permissions override the server's permissions. For example, if the server has read-only access to folder1, but user John Doe has read and write permissions to folder1, John Doe has those same permissions when he accesses folder1 through Enhanced File Transfer Server.

Windows NT permissions can be edited through the **Security** tab in the **Properties** of an object. On the **Security** tab, select **Permissions** to display and edit the permissions for the object. The appearance of this window 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. 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 also provides access levels that are simply 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." It does not contain any permissions.

LDAP

Using a LDAP database for authentication

LDAP (Lightweight Directory Access Protocol) is a protocol for accessing information directories on an LDAP Server. A typical LDAP server is a simple network-accessible database where user account lists are stored; and they include information about those users and what privileges each user has. Enhanced File Transfer Server supports Lightweight Directory Access Protocol (LDAP) databases for authenticating users. LDAP support on EFT Server allows you to authenticate users through connection to LDAP servers such as Novell eDirectory server, OpenLDAP, Sun ONE Server, Microsoft's Active Directory server, and Tivoli Access Manager. For more information on LDAP, see the Microsoft white paper Understanding LDAP.

Connecting to a LDAP Server

EFT Server needs specific information to successfully connect to the LDAP server. For host information, this includes the IP address or domain name and the port of the LDAP server, the base DN (Distinguished Name) which specifies the organizational unit (required with some systems) and any necessary domain components, the user filter EFT Server uses to query the LDAP server for users, and the attribute that denotes user names in the LDAP database.

Host Information

Host information about the LDAP server required by EFT Server includes:

- **IP address/Domain Name -** of the LDAP server
- **Port** of the LDAP server. This depends on the server you are connecting to, but the default is Port 389 (Port 636 for SSL connections).

- **Base DN -** The base distinguished name must include the domain components of the LDAP server. Some LDAP systems, such as Sun ONE Server and Microsoft's Active Directory server, require the organizational unit that houses the users on that LDAP server to be included in the BaseDN in order to allow users to successfully authenticate. The organizational unit is the parent object that contains the user objects. For example, if the classObject that holds user accounts is **person**, the hierarchical parent node/container could be the organizational unit **people**. If the organizational unit is required by your LDAP server, prepend it to the distinguished name.

  Example

  - With Organizational Unit:

    ```
    ou=people,dc=forest,dc=intranet,dc=gs
    ```

  - Without Organizational Unit:

    ```
    dc=forest,dc=intranet,dc=gs
    ```

- **User Filter** - This allows you to specify the filter that EFT Server uses to query the LDAP server for a list of users. The default setting is:

  ```
  objectClass=person
  ```

  This finds the LDAP entries that are part of the objectClass person; in other words, it retrieves the users on the LDAP server that belong to the person `ObjectClass`.

- **Attribute** - This allows you to specify the attribute from the queried list of users that denotes user names. Commonly used attributes are **cn** or **uid**.

User Information

User information defines how the client is authenticated. You can choose two binding methods:

- **Anonymous**
- **Simple** - This option requires a user name and password. Note that the user name must follow the syntax for the LDAP server that includes the Common Name and the Domain Components of your LDAP server's distinguished name. For example, the user name might be the following:

  ```
  cn=Manager,dc=forest,dc=intranet,dc=gs
  ```

Advanced Options

Additionally, you can specify SSL encryption, and the frequency the user list is refreshed.

Note:
When you use LDAP as the authentication method, EFT Server pulls the user account list and the authentication from the LDAP Server. Group lists, group membership, VFS Groups, and VFS User permissions are handled by EFT Server and stored in the local AUD and CFG files. These permissions must be configured and maintained with the EFT

Administrator or through the COM interface. GlobalSCAPE's professional services can help with migration of large groups with LDAP.

11

Protocols and Security

Protocols and security

Enhanced File Transfer Server supports the following protocols:

- FTP
- HTTP
- SSL/TLS
- HTTPS
- FTPS
- SSH
- SFTP

Enhanced File Transfer Server also provides data storage encryption based on OpenPGP.

FTP

The FTP protocol is an interactive file transfer mechanism that enables file transfers between Internet sites, or, more specifically, between two systems. It was created for transferring files independently of the operating system used, for example between a Macintosh and Windows PC. FTP's more notable features include handling for specific error situations and ensuring that a file sent from point A to point B will get there reliably.

FTP and Security

The FTP protocol specification (RFC 959) was published years ago when security was not a priority issue. As security became a concern, secure mechanisms such as SSL and TLS were adapted to help protect the FTP session from being intercepted or exploited. **GlobalSCAPE Enhanced File Transfer Server** provides security through the use of FTPS (using SSL/TLS).

HTTP

What is Hyper Text Transport Protocol (HTTP)?

HTTP is the communications protocol for establishing a connection with a Web server and transmitting HTML pages to the client browser or any other files required by an HTTP client application.

HTTP is a stateless request/response system. The connection is maintained between client and server only for the immediate request after which the connection is subsequently closed.

How does HTTP support in EFT Server differ from a typical Web Server?

EFT Server is primarily a file transfer server, not a Web server. This means it is not meant to "serve up" Web pages such as a typical Web server does for connecting HTTP clients (such as you Web browser). However there are provisions for transferring files in the HTTP protocol, which is a convenience when a connecting partner, customer or employee doesn't have an FTP client installed but does have an HTTP client or access to a Web page with HTTP PUT capabilities (usually an ActiveX control or Java applet).

When EFT Server is setup to allow HTTP file transfers, any HTTP client will be able to PUT (upload) or GET (download) files to the EFT server provided the client supports both of these HTTP commands. Most Web browsers only support the GET command or if they support the PUT command, they provide no interface for browsing to the user's local file system in order to select and upload (PUT) files onto the EFT Server. A few dedicated clients (such as CuteFTP Professional) and various thin clients (based on ActiveX controls or Java applets) support both PUT and GET capabilities, allowing these clients to transfer files to the EFT server in both directions.

HTTP Limitations in Enhanced File Transfer Server

- EFT allows you to customize messages sent by the server upon connection, login, maximum connections reached, and disconnect (for FTP sessions). Due to the nature of the HTTP protocol, custom login messages will not be displayed for connecting HTTP clients.
- Another limitation of HTTP is after a connection is established the browser will see the server's root folder instead of the user's home holder. A workaround is to setup a distinct Site for HTTP sessions.
- Certain syntax cannot be used when using some clients (such as a Web browser). When attempting to use an address in the format **http://test:test@localhost** the attempt fails and an invalid syntax error message appears. The protocol refuses to acknowledge this type of address and will not connect to the server. To connect, use the standard syntax: http://192.168.20.62, which prompts for the username and password.
- If you create an event rule that sends a notification email for each successful login event, an email is sent *every time* a user connected through HTTP changes directories.

This is a result of HTTP being a stateless protocol. This can result in a large volume of notification email even when performing typical directory browsing.

About SSL and TLS

Secure Socket Layer (SSL) is a protocol for encrypting and decrypting data across a secure connection from a client to a server with SSL capabilities. The server is responsible for sending the client a certificate and a public key for encryption. If the client trusts the server's certificate, an SSL connection can be established. All data passing from one side to the other will be encrypted. Only the client and the server will be able to decrypt the data. You can get a clearer idea of how SSL works by examining the representation of an explicit SSL transfer below.

GlobalSCAPE **Enhanced File Transfer Server** supports SSL for client and server authentication, message integrity, and confidentiality. You can configure GlobalSCAPE **Enhanced File Transfer Server**'s security features to verify users' identities, allows users to verify your identity and to encrypt file transfers. The key to understanding how SSL works is to understand the elements that take part in the process.

Elements that work together to establish a secure SSL connection

Client: The client needs to be an FTP client with SSL capabilities.

Certificate: Certificates are digital identification documents that allow both servers and clients to authenticate each other. A certificate file has a .crt extension. Server certificates contain information about your company and the organization that issued the certificate (such as Verisign or Thawte) while client certificates contain information about the user and the organization that signed the certificate. You can choose to either trust or distrust a certificate. In some cases, the client's certificate must be signed by the server's certificate in order to open an SSL connection.

Session Key: The client and the server use the session key to encrypt data. It is created by the client via the server's public key.

Public Key: The client encrypts a session key with the server's public key. It does not exist as a file, but is produced when a certificate and private key are created.

Private Key: The server's private key decrypts the client's session. The private key has a .key extension and is part of the public-private key pair.

Certificate Signing Request: A certificate signing request is generated each time a certificate is created. A certificate signing request has a .csr extension. This file is used when you need to have your certificate signed. Once the Certificate Signing Request file is signed, a new certificate is made and can be used to replace the unsigned certificate.

Authentication

Enhanced File Transfer Server supports two levels of authentication with SSL:

- High - The server is configured so that it contains a certificate, but does not require a certificate from the FTP client.
- Highest - The server is configured so that it provides a certificate and also requests a certificate from the client. The server compares the client certificate to a list contained in its Trusted Certificates database. The server either accepts or rejects the connection based upon a match.

Explicit versus implicit SSL

Netscape originally developed Secure Socket Layer (SSL) for secure Web browsing. When both a client and server support the AUTH SSL command security is accomplished through a sequence of commands passed between the **two** machines. The FTP protocol definition provides at least two distinct mechanisms by which this sequence is initiated: explicit (active) and implicit (passive) security.

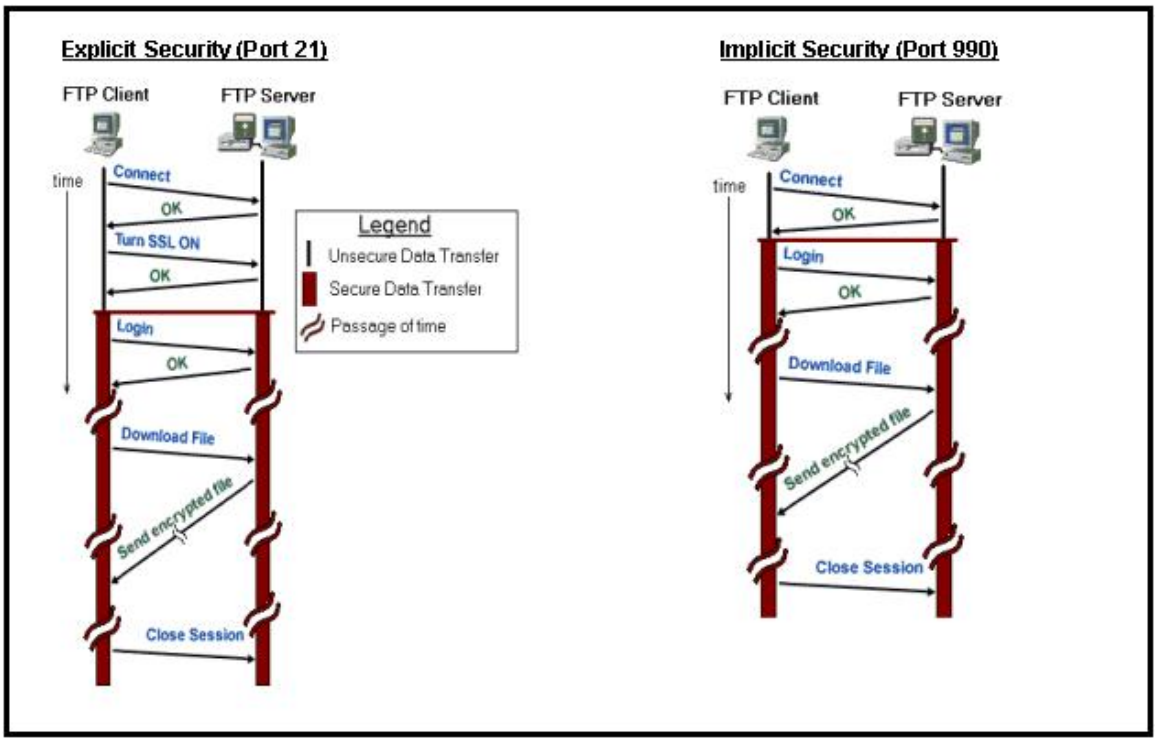
Explicit Security: In order to establish the SSL link, explicit security requires that the FTP client issue a specific command to the FTP server **after** establishing a connection. The default FTP server port is used. This formal method is documented in RFC 2228.

Implicit Security: Implicit security automatically begins with an SSL connection **as soon as** the FTP client connects to an FTP server. In implicit security, the FTP server defines a specific port for the client (990) to be used for secure connections.

> **Note:**
> Implicit SSL is discussed in various SSL drafts but is not formally adopted in an RFC. For strict compliance to standards, use the explicit method.

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

You can think of implicit security as "always on" and explicit security as "turn on." The following diagram contrasts implicit and explicit SSL connections.



FTPS

FTPS is an enhancement to standard FTP that uses standard FTP commands (and protocol) over secure sockets. FTPS adds SSL security in both the protocol and data channels. FTPS is also known as FTP-SSL and FTP-over-SSL. You may also see the term SSL used in conjunction with TSL. SSL has been merged with other protocols and authentication methods into a new protocol known as Transport Layer Security (TLS). Enhanced File Transfer Server employs SSL/TSL to perform FTPS and keep your data secure.

HTTPS

HTTPS is the protocol for accessing a secure Web server where authentication and encrypted communication is possible. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The default TCP/IP port of HTTPS is 443. The session is then managed by a security protocol. HTTPS encrypts the session data using the SSL (Secure Socket Layer) protocol ensuring reasonable protection from eavesdroppers and man-in-the-middle attacks.

Secure Socket Layer (SSL) is a protocol for encrypting and decrypting data across a secure connection from a client to a server with SSL capabilities. The server is responsible for sending the client a certificate and a public key for encryption. If the client trusts the server's certificate, an SSL connection can be established. All data passing from one side to the other will be encrypted. Only the client and the server will be able to decrypt the data. The SSL

protocol is the same protocol used in FTPS. Additional information on how SSL works is available under the FTPS section FTPS, SSL, and TLS.

Elements that work together to establish a secure HTTPS connection:

Client: The client must have SSL capabilities.

Certificate: Certificates are digital identification documents that allow both servers and clients to authenticate each other. A certificate file has a .crt extension. Server certificates contain information about your company and the organization that issued the certificate (such as Verisign or Thawte) while client certificates contain information about the user and the organization that signed the certificate. You can choose to either trust or distrust a certificate. In some cases, the client's certificate must be signed by the server's certificate in order to establish an SSL connection.

Session Key: The client and the server use the session key to encrypt data. It is created by the client via the server's public key.

Public Key: The client encrypts a session key with the server's public key. It does not exist as a file, but is produced when a certificate and private key are created.

Private Key: The server's private key decrypts the client's session. The private key has a .key extension and is part of the public-private key pair.

Certificate Signing Request: A certificate signing request is generated each time a certificate is created. A certificate signing request has a .csr extension. This file is used when you need to have your certificate signed. Once the Certificate Signing Request file is signed, a new certificate is made and can be used to replace the unsigned certificate.

Note:
In web pages that use HTTPS, the URL begins with 'https://' rather than 'http://'. HTTP clients should connect using standard requests (i.e. https://domain_name). EFT Server can be setup to provide connecting clients with a certificate and even require that the client provide a certificate upon connect (to further validate the client's identity).

SFTP

SFTP is an FTP-like protocol that uses SSH1 and SSH2 protocols to provide security. When clients make an SFTP (SSH2) connection with Enhanced File Transfer Server there are two components or layers involved: the Transport and Authentication layers.

Transport Layer

When users first attempt to connect to your SFTP site, the user's client software and the server determine whether the transmission should be encrypted or clear, compressed or uncompressed, what Method Authentication Code (MAC) to use, and what kind of encryption (cipher) to use.

Once the encryption method is chosen:

1. Enhanced File Transfer Server sends a public key to the client.
2. The client generates a session key, and encrypts it with the server's public key.
3. The client then sends the encrypted session key back to the server.
4. The server then decrypts the session key with its private key and from that time all transmitted data is encrypted with the session key.

Authentication Layer

After the Transport Layer is established, the server attempts to authenticate the client.

There are two methods Enhanced File Transfer Server can use for authentication.

- **Public Key Authentication Method: publickey**

  To use this method, the client will need a private key and public key. The public key is passed to the server. The server encrypts a random number with the public key and sends it to the client.

  1. The client asks the user for a passphrase to activate the private key.
  2. The private key decrypts the number and sends it back to the server.
  3. The server recognizes the number as correct and allows the connection.

- **Password Authentication Method: password**

  Using this method, the client sends its password to server. The client doesn't need to explicitly encrypt the password, because it will be automatically encrypted by the Transport Layer mentioned above. With this type of authentication, the connection will fail if the Transport Layer cannot encrypt the data.

After the encryption method is established, and authentication is complete, the two systems are ready to exchange secure data. The client sends a secured FTP connection along the encrypted data tunnel, the server responds and the user can then transfer files securely.

12

Automation

Automation

Enhanced File Transfer Server provides extensive automation functionality through commands, event rules, and a programmatic interface using COM APIs.

Custom Site Commands

Command-line executables can be configured to execute any program that the server has access from its filesystem. Open a program and provide a specific script or program to execute. You can give users permissions to execute the command, or you can configure an event rule to trigger a command.

Event Rules

Event rules enable task management automation. Event rules allow Enhanced File Transfer Server to carry out actions based on predetermined criteria. You can schedule routine tasks, or move a file automatically after a transfer. Event rules consist of an event trigger, optional conditions, and actions.

COM

Enhanced File Transfer Server's COM APIs allow you to program a unique or solution-specific interface and hook it right into the EFT Server's functionality.

Custom Site Commands

Creating a custom command

Custom commands allow connecting users to execute programs with command line arguments on the Server. The connecting user would issue the command directly from their FTP client.

To add a custom site command

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.

2. Select the Site you want to configure from the left-hand navigation tree.
3. Select the **Commands** icon in the left window.
4. In the right pane, click the **New** button and click the **Command** tab.

Note:
You may also launch a Commands Wizard from the toolbar icon represented by the command prompt (black box)

5. Enter the name of the command in the **Command** box. This is the command name that the connect user will issue in his/her FTP client.
6. Type in a **Description** that will help you identify the function of this command.
7. Choose the path to the executable by browsing, or typing the path in the **Executable** box.
8. Select the **Redirect output to client** or **Redirect output to system log** check box, depending on where you want the output of the command sent. You can select both or neither.
9. In the **Advanced** tab type the parameters (if any) that will be passed to the command line. The variable format used is %N%. You may specify multiple variables or hard coded values. (For Example: -c %1% %2%).
10. Select the **Require Parameter** check box if you want to force the FTP client to send a minimum number of parameters. If the box is checked specify the minimum number of parameters required in the text box. You can also write a message in the **Invalid parameter count message** text box that users will receive when the parameter number is not met.
11. Select the **Enable process timeout** check box if you want the EFT Server to return an error should the launched process fail to respond.
12. Enter the number of seconds you wish the server to wait before terminating the command.
13. Select the **Permissions** tab and verify that the appropriate users have permissions to run the newly created command.
14. Select **Apply**.

Custom command example

The following example command shows the configuration of a custom command from the perspective of both the **Enhanced File Transfer Server** and client. CuteFTP Professional will be the client used in this example, although any client that supports custom commands or raw FTP commands will work.

This command will compress an archive from the command line using CuteZIP's command line functions. Before attempting the following example, you will need to download and install CuteFTP Professional and CuteZIP. Both are available as a free 30-day trial and can be downloaded from www.globalscape.com.

Creating a custom command in Server

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. Select **Commands**.
4. In the right pane, click **New**. A new set of tabs appear at the top of the pane named **Commands**, **Advanced** and **Permissions**.

Commands tab

1. On the **Commands** tab, select the **Enable this command** check box.
2. In the **Command** field, enter the name **ZIP**.
3. In the **Description** field, enter **Compress selected files**.
4. In the **Executable** field, browse until you locate **C:\program files\globalscape\cutezip\cutezip.exe**.

> **Note:**
> You must have already installed CuteZIP on your computer.

5. Beneath **Output**, select the **Redirect output to client** check box.
6. Select the **Redirect output to system log** check box.

Advanced tab

1. Select the **Advanced** tab.
2. In the **Pass the following to the command** box, enter **-c %1% %2%**.
3. Select the **Require parameters** check box.
4. Select 2 in the **Command must have at least __ parameters** drop down box.
5. In the **Invalid Parameter Count Message** field, enter **Invalid Command! Usage Site ZIP [destination] [source]**.
6. Select the **Enable process timeout** check box.
7. Select **60** in the **Terminate Process if still running in __ seconds** drop down box.

Permissions tab

1. Select the **Permissions** tab.
2. Add the users or groups with permission to execute the command.

FTP Client Configuration

You must have CuteFTP Professional installed on your computer before you complete this section.

Creating a custom command for the FTP client

1. Start CuteFTP Professional and connect to Enhanced File Transfer Server.
2. Select **Tools** on the menu bar, find and expand **Custom Commands** then select **Edit Custom Commands**.

Note:
You must be connected to an FTP server in order for the **Commands** option to be available on CuteFTP Pro's menu bar.

3. Select the **New Command** icon and give your command a name.
4. Right-click the new command and select **Properties**.
5. For the **Label**, enter **ZIP Files on the Server**.
6. For the **Command**, enter **SITE ZIP %at[archive name] %ff** .

Note:
Commands must start with SITE and then the command name you used in Server.

7. Choose any key or key combination for the **Shortcut Key**.
8. Choose any icon for the **Toolbar Icon**.
9. Select the **Place on the Custom Commands toolbar** check box.
10. Select **OK** in the **Custom Commands Properties** dialog box.
11. Select **OK** to exit the **Commands** dialog box. Your custom command should now be enabled.

Testing the custom command

1. Start CuteFTP Pro and connect to Enhanced File Transfer Server.
2. Select **Tools > Custom Commands > New Command Name** from the menu.
3. Enter the item name to be zipped in the **Archive Name** window text box.
4. Select **OK**.
5. Monitor the output to the client log. You should receive various response messages indicating the progress of the archive.

Possible Error Situations

- If you repeat the hard coded parameters in both the client and server, such as SITE ZIP -c %at[archive name] %ff is used in the client, and -c %1% %2% in the sever, then the first parameter (-c) that the client sends will be used as %1%. So the resulting string would be: -c -c filename.ext. Therefore it is important to educate the user on the proper syntax and supply most of the hard coded parameters on the server side.
- If you do not add the user to the **Permissions** table in the **Permissions** tab on the server they will receive a "Permission Denied" error.
- Certain command line utilities that may show a Windows prompt or other dialog may not execute properly when called from the FTP Engine while it is running as a service. This is especially true when the service is being logged in from a Local System account.
- The server may return an error if the client provides the wrong number of parameters or invalid parameters. In order to limit security vulnerabilities to the

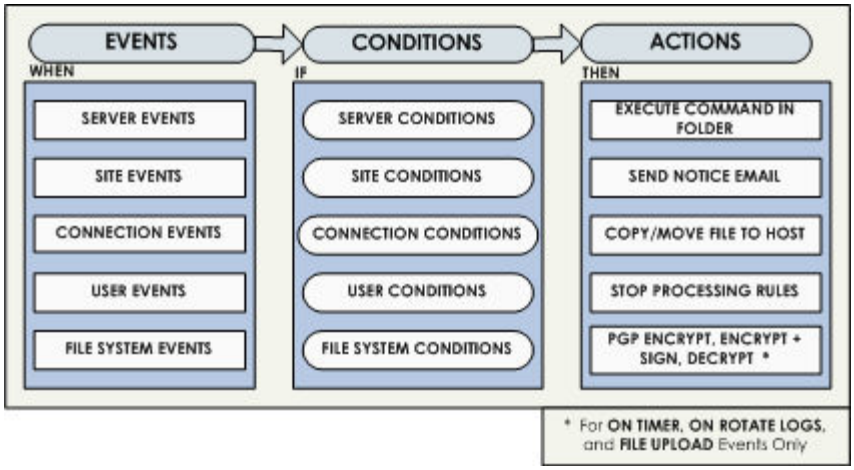
server, the server administrator should only allow limited access to commands that launch processes.

Event Rules

Event Rules

Event Rules automate management tasks. Define an event rule to trigger an action, or several actions, when specified criteria are met. For example, event triggers can be used to initiate additional activities after a file has been uploaded/downloaded. You can synchronize content across systems or provide an automatic response with an event rule, or you can trigger a custom command to run a custom application or script. You can specify

Event rules in Enhanced File Transfer Server consist of triggering **Events**, any optional **Conditions** affecting the event rule, and the resulting **Actions** that are carried out.



When multiple actions are defined for a single event rule, Enhanced File Transfer Server carries out the actions in the following order:

1. OpenPGP
2. Execute Custom Command
3. Move/Copy File
4. Email Notification
5. Stop Processing Rules

Warning:
It is possible to configure event rules that create infinitely recursive cycles. Since all event rules operate synchronously, a file upload event cannot be completed until all corresponding event actions are finished. This could lead to unpredictable server behavior due to conflicts with

shared access to the same files or deleting open files. Be careful not to create circumstances where such recursive cycles might occur. For file upload events, recursive cycles are not typical. It is recommended that you move files on the same server with the filesystem—not FTP.

Events

The following events can trigger actions:

Server Events

- **Service Stop**—When the **EFT Server** service stops.
- **Service Start**—When the **EFT Server** service starts.
- **Timer**—Execute a specified action one time or repeat at a specified interval.
- **Rotate Log**—When the current activity log closes and opens a new one.
- **Monitor Folder**—Monitor a specified folder then execute an action whenever a change is detected.

Site events

- **Site Stop**—When the site stops.
- **Site Start**—When the site starts.

Connection Events

- **User connect**—When a user connects to the site (this occurs before log in).
- **User connect failed**—When a user attempts to connect and fails (this can occur before log in).
- **User disconnect**—When a user disconnects from the site (this can occur before log in).

User Events

- **User account disable**—If the user account is disabled by the administrator or by the server.
- **User quota exceeded**—If the user has taken too much disk space on the server.
- **User logout**—If the user closes a session gracefully.
- **User login**—If the user logs in to the server.
- **User login failed**—If the user attempts an incorrect username or password.
- **User password changed**—If the user or administrator changes a user's password.

File System Events

- **Before download**—If a download is requested perform this first.
- **File delete**—If a file is deleted from the site.
- **File upload**—If a file is uploaded to the site.
- **File download**—If a file is downloaded from the site.
- **File rename**—If a file on the site is renamed.
- **File move**—If a file is transferred to another location.
- **Folder create**—If a folder is created on the site.
- **Folder delete**—If a folder is deleted from the site.
- **Folder change**—If a user navigates to a new folder on the site.
- **Upload Fail**—If an upload does not occur.
- **Download Fail**—If a download does not occur.

Conditions

Conditions allow you narrow the trigger definition an event rule. Conditions are optional: you do not have to define a condition on an event rule to make it trigger an action, but they do allow fine control over when an action may take place.

Server Conditions

You can only apply these conditions to
Server events.

- **If service is running** – The EFT Server service is currently running.
- **If log type** - The log type is a specific type.
- **If log location** - The log location matches a specific path.
- **If old log file path -** The log file path matches a specific path.
- I**f new log file path -** The log file path matches a specific path.
- **If old log file name -** The log file path matches a specific path.
- **If new log file name -** The log file path matches a specific path.

Site Conditions

You can only apply these conditions to **Site events**.

- **If site is running** – The site has already started and is currently running.

Connection Conditions

You can apply these conditions to **Connection events**, **User events**, and **File system events**.

If Remote IP

- a connection is made from a remote IP address that matches a predefined IP address or IP mask.
- a connection is made from a remote IP address that does NOT match a predefined IP address or IP mask.

If Local IP

- a connection is made to a local IP address that matches a predefined IP address or IP mask.
- a connection is made to a local IP address that does not match a predefined IP address or IP mask.

If Local Port

- a connection is made on a predefined port.
- a connection is made NOT on the predefined port.
- a connection is made on one of a predefined range of ports.
- a connection is made NOT on one of a predefined range of ports.

If Protocol

- an FTP/SSL/SFTP/HTTP/HTTPS connection has been made or is being used.
- a connection has been made or is being used that is NOT an FTP/SSL/SFTP/HTTP/HTTPS connection.

User Conditions

You can apply user conditions to **User events** and **File system events**.

If User

- the user account belongs to a specific group or set of groups.
- the user account does not belong to a specific group or set of groups.

If Login

- a user name matches a specific word.
- a user name does not match a specific word.
- a user name contains a specific string of characters.
- a user name does not contain a specific string of characters.

If Account Enabled

- a user account is enabled.
- a user account is disabled.

Back to top

If Settings Level

- the user belongs to a predefined Setting Level.
- the user does NOT belong to the predefined Settings Level.

if Full Name

- a user's name matches a predefined name.
- a user's full name does not match a predefined name.
- a user's full name contains a predefined string of characters.
- a user's full name does not contain a predefined string of characters.

if Description

- the user's description matches a predefined description.
- the user's description does NOT match a predefined description.
- the user's description contains a predefined string of characters.
- the user's description does NOT contain a predefined string of characters.

if Comment

- the user's comment matches a predefined comment.
- the user's comment does NOT match a predefined comment.
- the user's comment contains a predefined string of characters.
- the user's comment does NOT contain a predefined string of characters.

if Email Address

- the user's email address matches a predefined address.
- the user's email address does NOT match a predefined address.
- the user's email address contains a predefined string of characters.
- the user's email address does NOT contain a predefined string of characters.

if Phone Number

- the user's phone number matches a predefined phone number.
- the user's phone number does NOT match a predefined phone number.
- the user's phone number contains a predefined string of characters.
- the user's phone number does NOT contain a predefined string of characters.

if Pager Number

- the user's pager number matches a predefined number.
- the user's pager number does NOT match a predefined number.
- the user's pager number contains a predefined string of characters.
- the user's pager number does NOT contain a predefined string of characters.

if Fax Number

- the user's fax number matches a predefined number.
- the user's fax number does NOT match a predefined number.
- the user's fax number contains a predefined string of characters.
- the user's fax number does NOT contain a predefined string of characters.

if Home Folder

- the location of a user's home folder matches a predefined physical location.
- the location of a user's home folder does NOT match a predefined physical location.

if Home Folder is root

- the user's home folder is their root directory.
- the user's home folder is NOT their root directory.

if Quota Max

- the user's account has a size limit equal to a predefined size in Kilobytes.
- the user's account has a size limit less than or equal to a predefined size in Kilobytes.
- the user's account has a size limit less than a predefined size in Kilobytes.
- the user's account has a size limit NOT equal to a predefined size in Kilobytes.

- the user's account has a size limit NOT less than or equal to a predefined size in Kilobytes.
- the user's account has a size limit NOT less than a predefined size in Kilobytes.

if Quota Used

- the user has used a predefined amount (in kb) of allowed disk space.
- the user's filled disk space is less than or equal to a predefined amount (in kb) of allowed disk space.
- the user has used less than a predefined amount (in kb) of allowed disk space.
- the user has NOT used a predefined amount (in kb) of allowed disk space.
- the user's filled disk space is NOT less than or equal to a predefined amount (in kb) of allowed disk space.
- the user has NOT used less than a predefined amount (in kb) of allowed disk space.

if Invalid login attempts

- the user has attempted and failed to login a predefined number of times.
- the user's failed login attempts are less than or equal to a predefined number.
- the user's failed login attempts are less than a predefined number.
- the user has NOT attempted and failed to login a predefined number of times.
- the user's failed login attempts are NOT less than or equal to a predefined number.
- the user's failed login attempts are NOT less than a predefined number.

if User can change password

- the user has permission to change their own password.
- the user does not have permission to change their own password.

if Home IP

- the user's allowed IP address matches a predefined IP address or set of IP addresses.
- the user's allowed IP address does not match a predefined IP address or set of IP addresses.

if User can connect using SSL

- the user has SSL capability enabled.
- the user does not have SSL enabled.

if User can connect using FTP

- the user has configured a site and has an FTP account.
- the user does not an FTP site with an account configured.

if User can connect using SFTP

- the user has SFTP capability enabled.
- the user does not have SFTP enabled.

File System Conditions

You can apply file system conditions only to **File system events**.

if File Change

- a file is added, removed, or renamed.
- a file is NOT added, removed, or renamed.

if Physical Path

- the file or folder exists at a predefined physical location (the full folder path including the file name or wildcard).
- the file or folder does NOT exist at a predefined physical location (the full folder path including the file name or wildcard).

if Physical Folder Name

- the file or folder exists in a predefined physical folder (the folder path or wildcard without a file name).
- the file or folder does NOT exist in a predefined physical folder (the folder path or wildcard without a file name).

if File Name

- the file name matches a predefined string of characters and/or as specified by wildcard.
- the file name does not match a predefined string of characters and/or as specified by wildcard.

if Virtual Path

- the file or folder exists at a predefined virtual location and/or as specified by wildcard.
- the file or folder does NOT exist at a predefined virtual location and/or as specified by wildcard.

if Physical Destination Path

- the file or folder exists at a predefined physical location and/or as specified by wildcard.
- the file or folder does NOT exist at a predefined physical location and/or as specified by wildcard.

if Physical Destination Folder Name

- the physical folder name matches a predefined physical folder name and/or as specified by wildcard.

- the physical folder name does NOT match a predefined physical folder name and/or as specified by wildcard.

if Destination File Name

- the destination file name matches a predefined string of characters and/or as specified by wildcard.
- the destination file name does not match a predefined string of characters and/or as specified by wildcard.

if Virtual Destination Path

- the file or folder exists at a predefined virtual location (the full folder path including the file name and/or as specified wildcard).
- the file or folder does NOT exist at a predefined virtual location (the full folder path including the file name and/or as specified wildcard).

Condition parameters

You can apply particular properties to specific conditions for **Upload Fail** and **Download Fail** only in **File system events**, for **User Login Failure** and **User Logout** in **User events**, and for **User Connect Failure** in **Connection events**.

These are special conditions are defined by using the **specific reason** parameters found in the drop down menu in the **specify rule condition and action parameters** section.

File System Events

if Upload Fail (or Download Fail)

- the upload/download was aborted by User.
- access was denied.
- connection was closed.
- file was banned type.
- bandwidth quota was exceeded.

User Events

if User Login Failure

- the user account was disabled.
- an invalid password was used.
- the protocol used was not supported.
- the IP was restricted.
- there were too many connections per IP
- there were too many connections per site.
- there were too many connections per user.

if User Logout

- the FTP session was closed due to error.
- the FTP session was closed by a timeout.
- the FTP session was closed by the user.
- the IP address was banned.
- the maximum number of incorrect logins was reached.
- the TCP/IP connection was closed by a peer.
- the User was kicked by the administrator.

Connection Event

if User Connect Failure

- the IP address was rejected.
- the IP address was rejected and banned.
- there were too many connections per IP.
- there were too many connections per site.

Actions

Actions are the results of event triggers. You can specify multiple actions to occur from a single trigger.

Rule actions

- **Execute command** The custom command in a specific location is triggered.
- **Send Notification Email** An email message is sent to the address specified.
- **Copy/Move file** The designated file is automatically moved to another location.
- **OpenPGP encrypt/encrypt and sign/decrypt** The designated cryptographic action is performed on the file.
- **Download** The file is downloaded.
- **Stop processing more rules** No further rules are processed.

RULE ACTION POSSIBILITIES

ACTIONS / EVENTS	EXECUTE COMMAND IN FOLDER	SEND NOTICE EMAIL	COPY/MOVE FILE TO HOST	OpenPGP ENCRYPT, ENCRYPT + SIGN, DECRYPT	DOWNLOAD FILE FROM HOST	STOP PROCESSING MORE FILES
SERVER EVENTS						
Service Start	X	X				X
Service Stop	X	X				X
Timer	X	X	X	X	X	X
Rotate Log	X	X	X	X		X
Monitor Folder	X	X	X	X		
SITE EVENTS						
Site Start	X	X				X
Site Stop	X	X				X
CONNECTION EVENTS						
User Connect	X	X				X
User Disconnect	X	X				X
User Connect Fail	X	X				X
USER EVENTS						
Account Disabled	X	X				X
Quota Exceeded	X	X	X			X

Password Changed	**X**	**X**				**X**
User Login	**X**	**X**	**X**			**X**
User Logout	**X**	**X**	**X**	**X**		**X**
User Login Failure	**X**	**X**				**X**
FILE SYSTEM EVENTS						
File Delete	**X**	**X**	**X**			**X**
File Upload	**X**	**X**	**X**	**X**		**X**
Before Download	**X**	**X**	**X**			**X**
File Download	**X**	**X**	**X**			**X**
File Rename	**X**	**X**	**X**	**X**		**X**
Folder Create	**X**	**X**	**X**			**X**
Folder Delete	**X**	**X**	**X**			**X**
Folder Change	**X**	**X**	**X**			**X**
File Move	**X**	**X**	**X**	**X**		**X**
Upload Fail	**X**	**X**	**X**			**X**
Download Fail	**X**	**X**	**X**			**X**

Note:
When Enhanced File Transfer Server performs a copy/move action, the folder the files are moved from is left behind and emptied, but not deleted.

Note:
Enhanced File Transfer Server attempts up to 100 connections to move the file when a copy/move action is initiated. Users should consider configuring their FTP client or receiving server to permit this number of connections. The server can have at most 100 connections to each of 100 sites at any one time. Further, if the connection attempt fails there are no retry attempts. This is necessary because Event Rules are synchronous and must complete in a timely manner.

OpenPGP encryption/decryption

You can configure the server to use OpenPGP encryption for particular events. OpenPGP can be used with **Server Events** (the **On Timer** and **On Rotate Log** events), three **File System Events** (**File Upload, File Move,** and **File Rename**), and one User Event (**User Logout**). To use this action, the site must be configured for OpenPGP and appropriate keys generated.

To set up the server to use OpenPGP for particular event rules

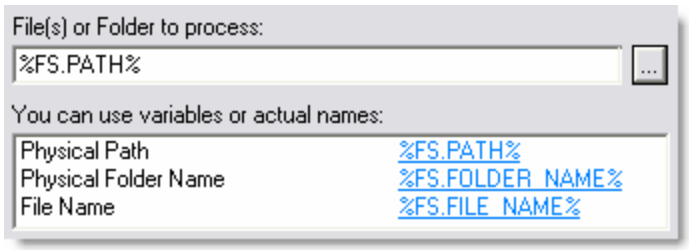
1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the event rule you want to configure.

Note:
This action applies only to the **On Timer**, **On Rotate Log**, **User Logout,** and **File Upload** events.) This example uses the **On File Upload** event.

3. Select **OpenPGP Encrypt, Encrypt + Sign, Decrypt** in the **Specify rule actions** in the right-hand pane. The rule parameters appear in **Specify rule condition and action parameters**.
4. Select one of the underlined elements in the **Specify rule condition and action parameters** area. The **OpenPGP Encrypt/Decrypt** dialog appears.
5. Select **Encrypt** or **Decrypt** from the drop-down menu.
6. Verify there is at least one key selected in the **Encrypt/Decrypt** pane. If you designated a default key for the site, that key will be displayed. If there is no default key, the right pane will be blank.
7. Add or remove keys from the **Encrypt/Decrypt** pane using the arrow keys located between the **OpenPGP Key List** pane and the **Encrypt/Decrypt** pane.

Arrow	What it does...
>	Moves the selected key to the 'use' list.
<	Removes the selected key from the 'use' list.
>>	Adds all keys to the 'use' list.
<<	Removes all keys from the 'use' list.

8. If you want the encrypted transmission signed, select **Sign using the following key**. The default key is displayed. Use the drop-down menu to select a different key. This option is not available for decryption.



9. Select the file or folder to process. The default target file is already entered. To change the selection, you can select a variable or use actual file/folder names. The button at the right of the text box allows you to browse to a file or folder.
10. Select **OK** to close the window and apply the parameters.

Copy/Move

You can configure the server to copy or move files to a specific location using a particular protocol whenever certain events occur. You must provide **EFT Server** with connection information (protocol and login details) and file information (source path and destination path).

> **Note:**
> The copy/move action can be applied to all File System events, User Events 'Quota Exceeded,' 'User Login,' 'User Logout,' and Server Events 'On Timer' and 'On Rotate Log.') This example uses the **On File Upload** event.

To set up the server to copy/move files

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. Expand **Event Rules**.
4. Select the event rule you want to configure.
5. Select **Copy/Move file to host** in the **Specify rule actions** in the right-hand pane. The rule parameters display in the **Specify rule condition and action parameters** area.
6. Select one of the undefined parameters in the **Specify rule condition and action parameters** area. The **File Copy Options** dialog appears. The **Connection Options** tab is the default display.
7. Select the **Protocol type** for the connection. Optional selections are available from the drop down menu. The port for the selected protocol changes automatically.
8. Enter the IP or host address in **host address**.
9. In the **Authentication** section, enter the user name and password needed to establish the connection.

- Select **Use connected client's user name and password to authenticate** if you are configuring an event rule that must authenticate multiple users. This option is only available if the Site level setting to allow usernames and passwords as replacement variables is enabled.
- If SFTP has been selected as the protocol type, enter the public key file path, the private key file path, and the key passphrase.

10. Select the **Target File** tab to display the file source and file destination options.
11. Select the **Source Path** option, the event target file (for example, log files for the On Rotate Log event) or a specified file.
12. Select if you want the source file to be deleted after the upload is successful.
13. Select the **Destination Path** option/location.
14. Select **Apply**.

Using wildcards with event rule actions

The OpenPGP action and the Copy/Move action support the use of wildcards. This is useful for event rules that batch process groups of files. Standard Windows/DOS format wildcards are used, such as *.*file extension , search term*.???, *search term* ?.*, *.*, and so on. This functionality is particularly useful with the Timer event.

Wildcards with OpenPGP

In the OpenPGP action configuration dialog, the **File to Process** field supports wildcards. Each matching file is acted upon according to the action definition.

Wildcards with Copy/Move

In the Copy/Move action configuration dialog, the source path field **Upload specified file** under the Target File tab supports wildcards. When a wildcard is specified here, the Destination path field specifies the target folder that each matching file is moved or copied

to. The files moved or copied into the destination file are given the same name as the files from the source.

Example

Source:

```
c:\test\*.txt
```

Destination:

```
/%FS.FILENAME%
```

Here, each "*.txt" file that is uploaded goes to "/", with a matching file name. Note that the destination file name is not overwritten.

Configuration Notes

- If the **source** of an action is specified as a wildcard without any path information, the path defaults to the folder with the event rule that triggered this action (for example, there is a "%FS.PATH%" variable for an **On Upload** event.) If there is no folder like that available—for example, if the event is an **On Timer** event—the current working directory of the application is set as the source of the wildcard patterns. Typically, that is the installation directory of the application.
- When you define a wildcard in the source path for a copy/move action and the protocol type is set to Local (Local Files or LAN), EFT Server respects Windows path syntax:

  Source:

  ```
  c:\Work\Today\*.*
  ```

  Destination:

  ```
  g:\Backup\Work\Today\
  ```

  You can also use `\\Work,` if appropriate.
- The Destination Path (Upload event target file as:) ignores any path information you enter after the trailing backslash. So if you enter `g:\Backup\Work\Today`, EFT disregards "Today" and executes the move/copy into `g:\Backup\Work\`.

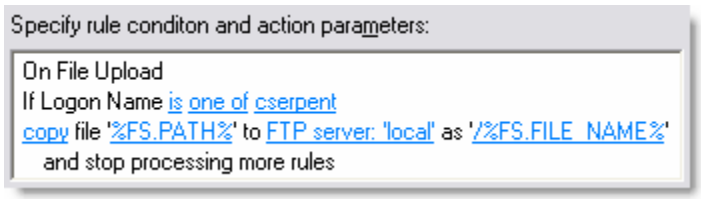
Note:
Take care to test an event rule using a wildcard before you deploy it. For example, if you do not define the source path appropriately when a wildcard is used, it is possible to set up an action that moves all the files out of a user's c:\windows directory, which is most likely an undesired result.

Stop Processing

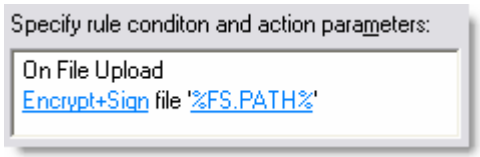
Stop Processing ends any further rule processing. The Stop Processing action is part of the process that is used in the development of how event rules operate. The example below

shows three rules that are triggered with an On Upload event. The stop processing action causes the other two processes in this example to stop.

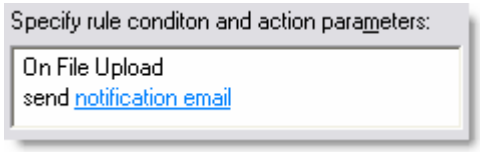
Rule 1



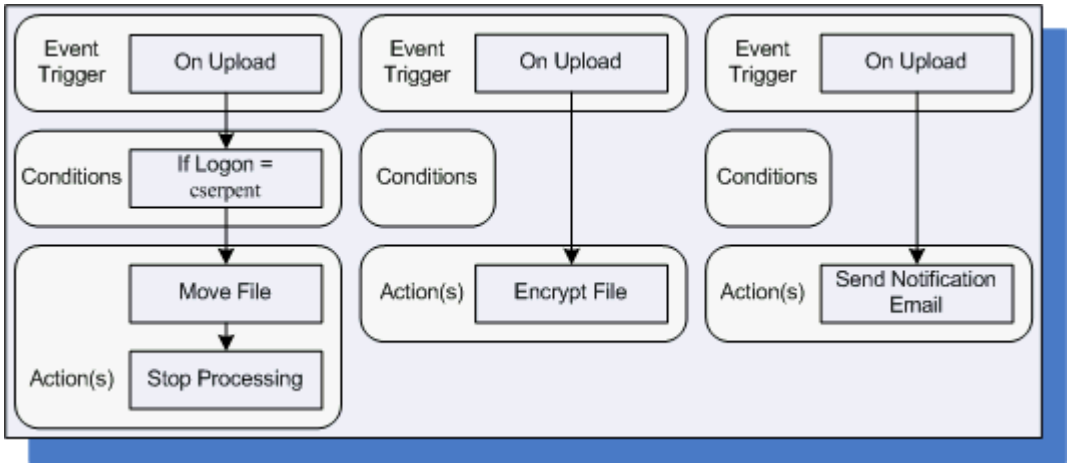
Rule 2



Rule 3



This diagram shows how the logic is executed:



Based on these rules all users except *cserpent* will have files encrypted and receive an email notification when a file is uploaded.

Download

You can configure the server to copy or download from a specific location to a specified local folder using a particular protocol whenever certain events occur. You must provide **EFT Server** with connection information (protocol and login details) and file information (source path and destination path).

Note:
The download action can only be applied to the On Timer Server event.

To set up the server to download files

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. Expand **Event Rules**.
4. Select the Timer event rule.
5. Select **Download file from host** from **Specify actions** The rule parameters display in the **Specify rule condition and action parameters** area.
6. Select one of the undefined parameters in the **Specify rule condition and action parameters** area. The **File Downloads Options** dialog appears. The **Connection Options** tab is the default display.
7. Select the **Protocol type** for the connection. Optional selections are available from the drop down menu. The port for the selected protocol changes automatically.
8. Enter the IP or host address in **host address**.
9. In the **Authentication** section, enter the user name and password needed to establish the connection.
    - Select **Use connected client's user name and password to authenticate** if you are configuring an event rule that must authenticate multiple users. This option is only available if the Site level setting to allow usernames and passwords as replacement variables is enabled.
    - If SFTP has been selected as the protocol type, enter the public key file path, the private key file path, and the key passphrase.
10. Select the **Target File** tab to display the file source and file destination options.
11. Select the **Source Path** option, the event target file or a specified file.
12. Select if you want the source file to be deleted after the upload is successful.
13. Select the **Destination Path** option/location.
14. Select **Apply**.

Creating, Editing, and Disabling event rules

To Create an Event Rule

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.

3. Select **Configuration > Create New Event Rule** from the menu. The **Create New Rule** window appears.
4. Enter a name for the rule.
5. In **Should be applied when**, select the event you want as a trigger.
6. Select **OK**. The **Create New Rule** window closes and the conditions and actions available for your rule are displayed in the right-hand pane.
7. Optionally select any **conditions** for the event rule.
8. Specify the action(s) the event rule triggers.
   - Choose **Execute command in folder** to run any custom command you have created for the site.
   - Choose **Send email notification** to send an email message to the address you entered in the server **SMTP Configuration** tab, and optionally send a message to a user.
   - If you want other rules for the event to be ignored if this rule is met, select **Stop processing more rules**.
   - Choose **Copy/Move file to host** to place files in an appropriate folder or location.
   - Choose **OpenPGP Encrypt, Encrypt + Sign, Decrypt** to encrypt a file. Note that this action can only be selected for On Timer, On Rotate Log, or On File Upload events.
9. In **Specify rule condition and action parameters**, select the blue and red text links to toggle behavior and select executables, email addresses or define file paths used in definition of the event rule. Enhanced File Transfer Server does not save the rule unless it is adequately defined.
10. Select **Apply** to enable the rule.

Note:
Red links in **Specify rule condition and action parameters** indicate parameters that have not yet been defined. They must be defined to save the rule.

To edit an event rule

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. From the left-hand navigation tree, select Event Rules under the Site you want to configure.
3. The Event Rules for that Site display in the right-hand pane.
4. Select the event rule you want to change.
5. Select **Edit**. The event rule's details appear in the right-hand pane.
6. Make any desired changes to the event rule.
7. Select **Apply**.

To disable an event rule

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. From the left-hand navigation tree, select Event Rules under the Site you want to configure.
3. The Event Rules for that Site display in the right-hand pane.
4. Clear the check box next to the event rule you want to disable.
5. Select **Apply**.

To re-enable an event rule

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. From the left-hand navigation tree, select Event Rules under the Site you want to configure.
3. The Event Rules for that Site display in the right-hand pane.
4. Select the check box next to the event rule you want to re-enable.
5. Select **Apply**.

To delete an event rule

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. From the left-hand navigation tree, select Event Rules under the Site you want to configure.
3. Select the event rule you want to delete.
4. At the far right of the Administrator interface, click **Delete**. A **Delete Rule** dialog appears.
5. Select **Yes**. The rule is deleted from the site.

Reorder Event Rules

Event rule actions can be reordered to specify a chain of events when the event rule triggers.

Action Parameters

As you add actions to an event rule, they appear at the bottom of the action parameter list. You can reorder them by clicking the up and down arrows next to the parameter. You cannot change the stop processing more rules parameter; it is always last.

> **Note:**
> You cannot add more than one parameter of each action type. For example, you cannot add two PGP actions to the same event rule.

Action failure options

You can define an additional action if another specified action fails to occur. This allows you to gracefully stop a failed action, or to schedule or program another action if the event action fails.

Action failure parameters

For example, if a copy action fails, you can set up an email notification to inform someone that the file copy failed.

To specify a failure action

1. In the Specify action parameters dialog, click the plus sign next to the action parameter you want to specify a failure action for.
2. Select the failure action and configure if necessary.

Using an event rule to trigger a custom command

You can configure the server to automatically run custom commands when specific events occur. You can find a list of the events you can use as triggers in Server events and conditions.

To automatically start a custom command

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. Select **Event Rules**.
4. In the right pane, select **New**. The **Create New Rule** dialog appears.
5. Enter a name for the rule.
6. Select the event trigger from **Should be applied when:**
7. Select **OK**. The **Create New Rule** window closes and the new rule is displayed in the right-hand pane.
8. If you need to apply any conditional behavior select it from **Specify rule conditions**.
9. From **Specify rule actions**, select **Execute command in folder**.
10. From **Specify rule condition and action parameters**, choose the red link **select**. The **Custom Command** window appears.

> **Note:**
> Red links in **Specify rule condition and action parameters** indicate parameters that have not yet been defined. They must be defined to save the rule.

11. Select the desired command from **Select command**.
12. Optionally include any parameters for the command in **Specify command parameters**. You can also select the items in the **Available Tags** list to add them as parameters.
13. In **Specify command working folder** type the path or click the yellow Browse button to choose the folder where the custom command executable resides.
14. Select **OK**.
15. At the top of the right pane, make sure **Rule Enabled** is selected.

Customizing event rule email notifications

You can create a custom email message for every event rule you define.

To customize an event rule email message

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. Expand **Event Rules**.
4. Select the event rule with the message you want to customize.
5. In the middle of the right-hand pane, make sure **Send notification email** is selected.
6. At the bottom of the right-hand pane, select the blue **notification email** text. The **Edit Mail Template** window appears.

7. In the **Subject** box, type any text you would like as a subject.
8. In the **Body** box, type any text you want.
9. In the **Available Tags** box, click any property you want to insert in the email message. The text surrounded by per cent signs signifies text that will be replaced by the server with specific information about the event, the user, or the connection.
   - If you just want the specific text in your email message, click the text surrounded by the per cent sign in the right column of the **Available Tags** box.
   - If you want the specific text, and the explanatory text before it, click the text in the left column of the **Available Tags** box.
10. If you want to send a copy of the message to the involved user select the **CC Mail Notification to user** check box. In order for the **CC Mail Notification to user** check box to be available your rule must be based on a **User Event**. To base a rule on a **User Even**t, create a new rule and select an option from the **User Event** list.
11. Select **OK**.

Note:
Red links in **Specify rule condition and action parameters** indicate parameters that have not yet been defined. They must be defined to save the rule.

Note:
You can edit the email messages even if you are not familiar with HTML. If you delete all the HTML tags the message is sent as a plain text message.

To send email as plain text

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the Site you want to configure from the left-hand navigation tree.
3. Expand **Event Rules**.
4. Select the event rule with the message you want to customize.
5. In the middle of the right pane, make sure the **Send notification** email check box is selected.
6. In the bottom of the right pane, click the blue **notification** email text. The **Edit Mail Template** window appears.
7. In the **Body** box, delete all the HTML tags.
8. Select **OK**.

Configuring SMTP email notification

You can configure the server to send email alerts whenever certain events occur. You must provide **EFT Server** with the address for an outgoing mail server, an address for the administrator, and other details.

To set up the server to send email notifications

1. Select the **Server tab** in EFT Administrator and select a server the server you want to configure.
2. Select the **SMTP Configuration** tab from the right-hand workspace.
3. In **SMTP Server Address**, enter the address of the mail server the EFT Server will use to send outgoing messages.
4. In **SMTP Server Port**, enter the port number where the mail server accepts messages. The standard is **25**.
5. If EFT Server can connect to the mail server without a log in, leave the **Server requires authorization** check box clear and skip to step ten. If the mail server requires a user name and password from the EFT Server computer, select the **Server requires authorization** check box and continue with step eight.
6. In the **Login** box, enter the user name needed to connect to the mail server.
7. In the **Password** box, enter the password needed to connect to the mail server.
8. In the **Name** box of the **Send Messages FROM** group, enter any name you would like for the "From Name" field.
9. In the **Address** box of the **Send Messages FROM** group, enter any address you would like for the "From Address" field.
10. In the **Name** box of the **Send Messages TO** group, enter the name of the server administrator, or any name you wish.
11. In the **Address** box of the **Send Messages TO** group, enter the email address of the person that should be notified of server events.
12. Select **Apply**.

Note:
The first name/address pair entered is automatically entered into the "To:" field in the send email notification action dialog. Subsequent name/address pairs are automatically entered into the "CC:" field in the send email notification action dialog.

COM

COM APIs

You can interact directly with EFT Server from your own custom applications using any COM enabled programming language such as Visual Basic (VB), Java, or C++. You can create a script with the development IDE of your choice. To create a new script file, you must be familiar with programming concepts and should have experience with COM enabled programming languages.

For more information see GlobalSCAPE's *EFT COM API Reference Manual.*

13

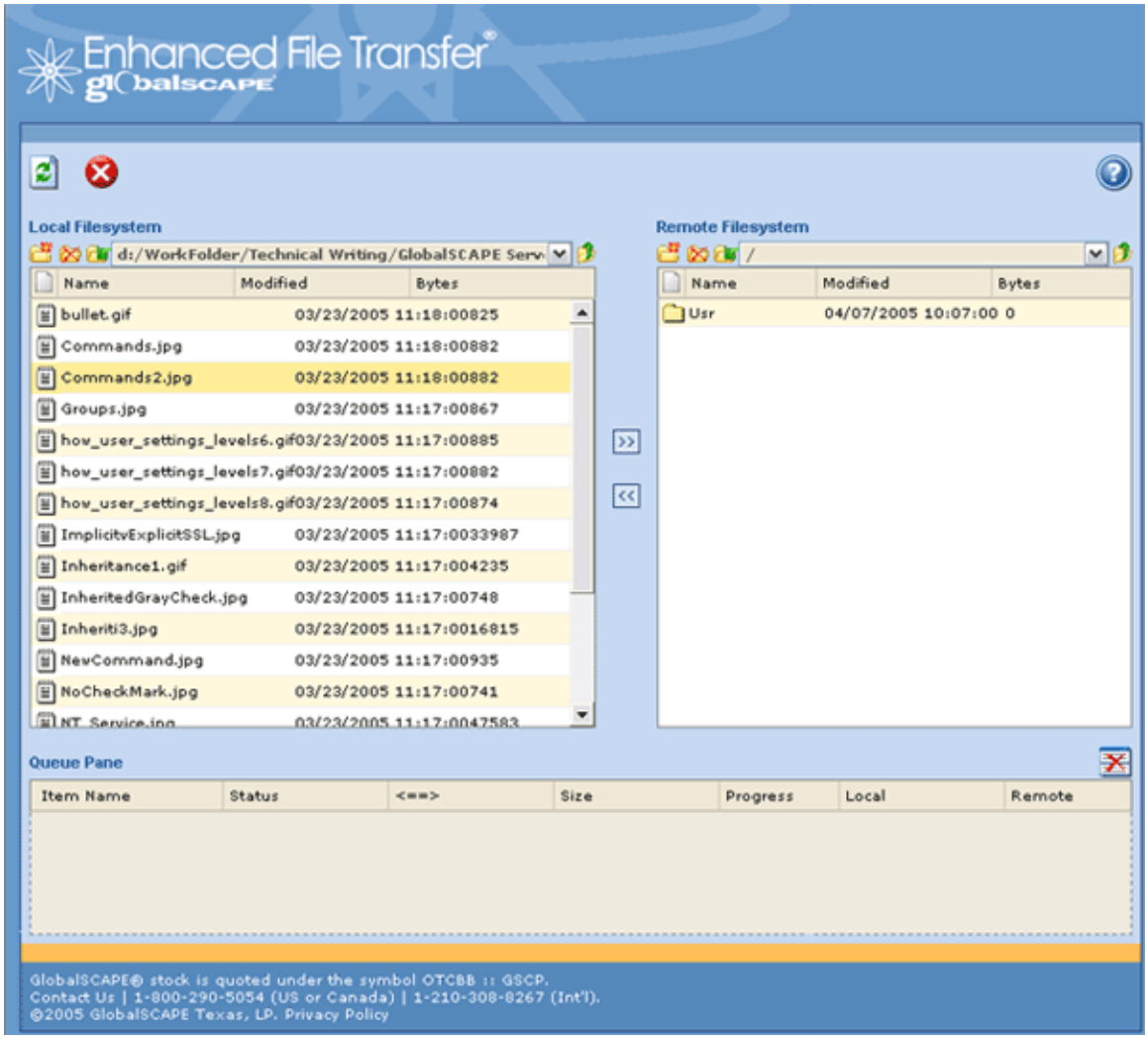
EFT Web Transfer Client

EFT Web Transfer Client

Enhanced File Transfer optionally includes the EFT Web Transfer Client, which is a browser based file transfer client that allows users to upload and download files to an EFT server using a connected web browser. If you have a license for the client, it deploys automatically if it is enabled for the user in the EFT Administrator. It allows your users to transfer files over HTTP or HTTPS using a web browser. The client works in most modern, major web browsers: Internet Explorer, Firefox, Mozilla, Netscape, Safari, Konqueror.

Overview of the client

The EFT Web Transfer Client consists of three work areas. The **Local Filesystem** displays files on the user's computer. The **Remote Filesystem** displays the files accessible to the user on the EFT Server. The **Queue Pane** displays the items being transferred.



EFT Web Transfer Client

Session status

The EFT Administrator shows how many session licenses are currently in use and how many remain available.

To check EFT Web Client status:

1. In EFT Administrator, select the **Status** tab. You should be connected to the server.
2. Select the site you want to monitor.
3. The number of sessions in use and the number remaining are displayed in the right-hand status pane.

Enable user access to the EFT Web Transfer Client

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. From the left-hand navigation tree, select the **User** or **User Setting Level** you want to enable access for.
3. In the right pane, select the **Security** tab.
4. Select **Allow use of Web Transfer Client for HTTP(S) transfers**.
5. Select **Apply** to save your changes.

Note:
HTTP or HTTPS must also be enabled. It is highly recommended that HTTPS is used if security is a concern.

The EFT Server allows users concurrent access to the EFT Web Transfer Client up to the number of your available licenses. If a user attempts to access the client when the maximum number of licenses is in use, the upload form loads instead.

Configuration Notes for EFT Web Transfer Client

- Turn off Auto-ban flood sensitivity to allow users to successfully connect using the transfer client.
- The client needs cookies enabled on the user's browser for the applet to work correctly. Note that cookies work on IP addresses or full domain names -- not "localhost," so if you are testing the system before you deploy it for customer use, do your tests using full DNS names or the IP address that you expect the customers to use.
- Concurrent licenses are based on sessions. For example, if a single user opens a browser window and connects to EFT Server, then opens another browser window and connects again, that counts as two license seats.
- If a user has multiple sessions open and you want to free up licenses, stop and restart the site. This resets the license count. Note that this also disconnects everybody who is connected; they must reestablish their session.

Client Usage Notes

- Users cannot transfer folders; only single files and groups of files. It is possible to create a folder and then transfer the entire contents of another folder from one computer to another. For example, if there is a folder on the local hard drive called "Accounts" and you want a folder exactly like it on the EFT Server, create a folder "Accounts" on the server, then copy the contents from the "Accounts" folder on your hard drive to the new "Accounts" folder just created on the EFT Server.
- Transfers cannot be resumed after they are stopped.
- When the browser is closed, the session expires within 5 minutes.

- Sessions disconnect after 5 minutes of inactivity. Inactivity involves server-side activity such as transfers, browsing the remote pane, creation, deletion, or the renaming of remote files.
- If a session times out, the browser must be refreshed to connect with a fresh session. If the session times out, you can still browse on the Local Filesystem (that is, on your computer), but you will not be able to do anything on the Remote Filesystem, such as rename files or folders, transfer files, etc.
- The EFT Web Transfer Client is licensed on a concurrent use basis. If the user logs into multiple browser windows, it will tie up a license seat for every browser instance that is logged in. You may want to inform your users not to use more seats than they need.

XCRC integrity checking in the EFT Web Transfer Client

The EFT Web Transfer Client can validate the integrity of files transferred to and from EFT Server. EFT Server must have XCRC enabled to take advantage of this feature.

When the EFT Web Transfer Client transfers a file to or from the EFT server, it automatically queries the server for the Cyclical Redundancy Check (CRC32) value of the file then compares it to the CRC value for the local file. If they match, the transfer is reported as successful. If they do not match, the Queue pane reports "CRC Failure." The user can then retry the transfer if necessary. The client does not automatically retry the transfer.

Rebranding the Web Transfer client

The EFT Web Transfer Client can be easily rebranded to suit your needs. Its appearance is controlled by a .css file that is placed in the EFT installation directory:

```
%install location%/EFTClient/eftstyle.css
```

The image files in the same directory (EFTClient) can be substituted for any you wish as well.

> **Note:**
> Make a backup copy of the stylesheet and the image files before you make any changes to them.

Trial use of EFT Web Transfer Client

The client is available for use during 30-day trials of EFT Server. The trial allows 5 concurrent sessions. After the trial has expired, a license must be purchased to resume use of the client.

EFT Web Transfer Client Licensing

Use of the client requires the purchase of a license. Licenses for the client are for concurrent users; any number can have access, but only the number specified by the license can use the client concurrently. Session use is cookie based. If the license number is exceeded, the user is automatically directed to the form upload page with an explanatory error message.

System requirements for the web transfer client

- Java 1.4.2 (J2SE) or better is required for the computer running the EFT Web Transfer Client.
- The browser running the client must have Javascript enabled
- The browser running the client must have cookies enabled

Note:
The user of the client must accept a security prompt (they should choose "Yes") to enable the Java applet that drives the client application.

Supported web browsers

The EFT Web Transfer Client has been tested for use with the following browsers:

Windows 2000, XP:

- Internet Explorer 6.0
- Firefox 1.0.3
- Mozilla 1.7.7
- Netscape 7.2
- Opera 8.0

Linux:

- Firefox 1.0.3
- Mozilla 1.7.7
- Konqueror 3.3.1

Mac OS X:

- Safari 1.2.4
- Firefox 1.0.3

Note:
Drag and drop works only with IE 6.

Checking Java runtime versions

To see which Java runtime version a browser is using:

- **Internet Explorer**

Select Tools > Sun Java Console. The plug-in version number displays at the top of the console.

- **Firefox**

  Browse to **about:plugins**.
- **Mozilla**

  Browse to **about:plugins**.
- **Safari**

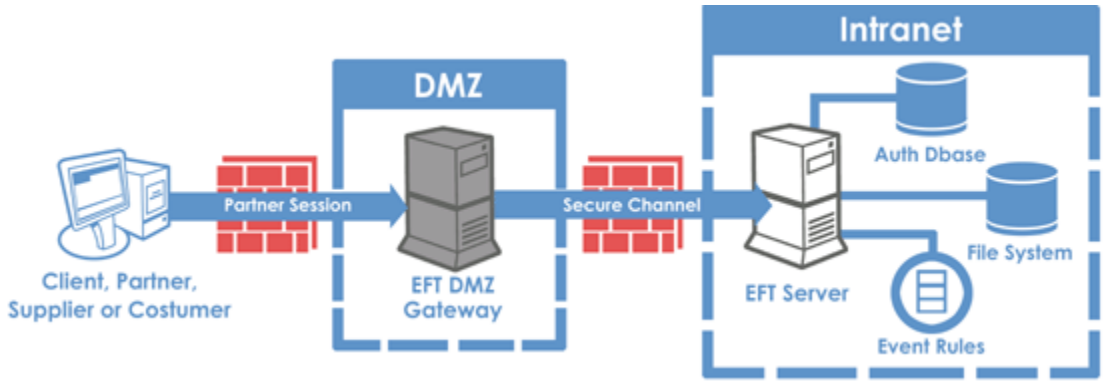
  From the menu, select **Help > Installed Plugins**.

14

DMZ Gateway

DMZ Gateway

The DMZ Gateway is designed to reside in the demilitarized zone and provide secured communications with EFT Server behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ. EFT Server establishes peer notification channels with the DMZ Gateway, and the DMZ Gateway sends all data only through these channels. The peer notification channel acts as a proxy for all transmission through the DMZ Gateway; the result is that EFT server can be set up exactly the same way, and behaves just as if it were in the DMZ, but it's actually safely behind the internal network firewall. The peer notification channel replaces the traditional inbound socket connection method for socket communications.



DMZ Gateway

Peer Notification

EFT Server and DMZ Gateway communication over a peer notification channel, which is a raw socket connection that uses a proprietary binary protocol to handle notifications from the Gateway to the DMZ. Requests for client connectivity to the DMZ Gateway are forwarded to the EFT Server; the EFT Server then opens connections back to the DMZ Gateway server using a raw socket connection; the gateway then pipes all data to the internal server using this socket without any translation. Thus, if the client is using HTTPS, then HTTPS traffic goes over that pipe.

Enable the DMZ Gateway

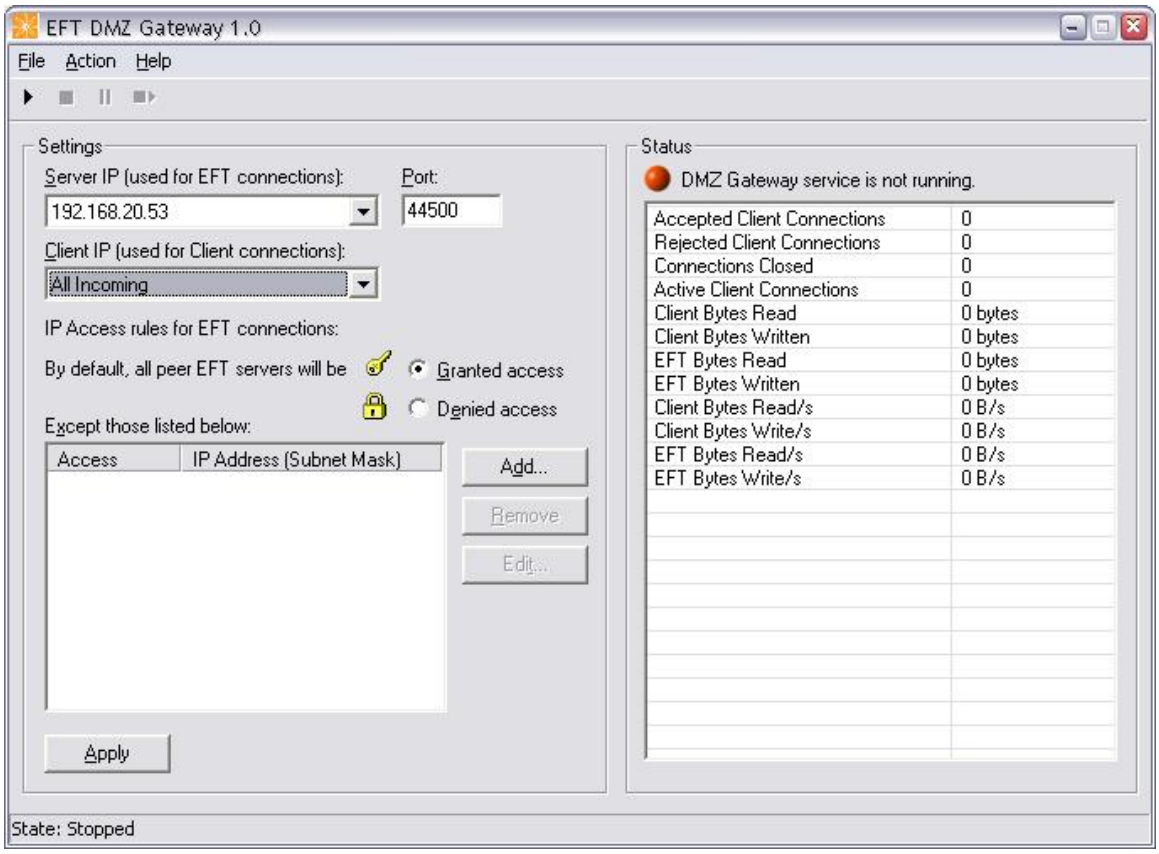
To enable the DMZ Gateway

1. From the EFT Administrator, select the **Server** tab. You should be connected to the EFT server engine.
2. Select the site you want to connect with the DMZ Gateway.
3. Select **Gateway**.
4. In the right pane, select the **General** tab.
5. Select **Enable Gateway**.
6. Enter the IP address and the port number of the DMZ Gateway you are connecting to.
7. In the right pane, select the **Ports** tab.
8. Select the ports you want the DMZ Gateway to listen to. This is a separate configuration from the ports EFT Server listens to, set from the Connection Options tab at the site level. For example, you can use port 21 for FTP traffic for EFT Server, but port 1465 for FTP traffic through the DMZ Gateway.
9. Select **Apply** to make the changes.
10. Re-establish a new connnection with any connected EFT Server by stopping and restarting connected sites.

DMZ Gateway interface

Configure the DMZ Gateway

The DMZ Gateway should be configured before you enable the gateway from the EFT Administrator. Configuration of the server is done from the DMZ Gateway interface.



DMZ Gateway

Settings

Server IP

The Server IP determines the IP addresses the DMZ Gateway uses for connections with EFT Servers. Select a specific IP address or choose **All Incoming**.

Port

The port number determines which port EFT Server and DMZ Gateway uses to communicate with each other. The default is 44500.

Client IP

The Client IP determines the IP addresses the DMZ Gateway allows for client connections. Select a specific IP address or choose **All Incoming**.

IP access rules for EFT Servers

By default, all IP addresses are granted access to the server. There are two ways to limit which IP addresses can connect to the DMZ Gateway:

- Grant access to only one specific IP address or a range of IP addresses.
- Deny access to one specific address or a range of addresses.

To grant access by IP Address

1. Select the **Denied Access** radio button.
2. Click the **Add** button. The **IP Mask** dialog box appears.
3. Enter the IP address or range of IP addresses that WILL have access to your FTP site. You can also use wildcards to select ranges of IP addresses.
4. Select **OK**.
5. Select **Apply** to save your changes.

To deny access by IP address

1. Select the **Grant Access** radio button.
2. Select the **Add** button. The **IP Mask** dialog box appears.
3. Enter the IP address or range of IP addresses that will *not* have access to your FTP site. You can also use wildcards to select ranges of IP addresses.
4. Select **OK**.
5. Select **Apply** to save your changes.

Status

The Status pane shows various statistics that DMZ Gateway monitors.

The top line indicates if the DMZ Gateway is connected, not connected, running, or not running.
Other statistics displayed include:

- Active Sites
- Accepted Client Connections
- Rejected Client Connections
- Connections Closed
- Active Client Connections
- Client Bytes Read
- Client Bytes Written
- EFT Bytes Read
- EFT Bytes Written
- Client Bytes Read/s
- Client Bytes Written/s
- EFT Bytes Read/s
- EFT Bytes Written/s

Note:
When you make changes to DMZ Gateway, you must stop and restart any site connected to the gateway from EFT Server.

Manage the DMZ Gateway

You can start, pause, restart, or stop DMZ Gateway from the control toolbar or from the menu. Note that these actions are performed on the DMZ Gateway server service.

To start the DMZ Gateway

- From the DMZ Gateway menu, select **Action > Start.**

To pause the DMZ Gateway

- From the DMZ Gateway menu, select **Action > Pause.**

To restart the DMZ Gateway

- From the DMZ Gateway menu, select **Action > Restart.**

To stop the DMZ Gateway

- From the DMZ Gateway menu, select **Action > Stop.**

Note:
When you make changes to DMZ Gateway, you must stop and restart any site connected to the gateway from EFT Server.

15

Troubleshooting

IP conflicts

If you already have an FTP server running and attempt to configure EFT Server to listen on the same IP and port, you will receive an error message stating that you cannot start that site. This is by design: you are not allowed to have two services listening on the same IP and port.

Either stop the other FTP server or configure the servers to listen on different IP addresses or ports.

If you have Microsoft Internet Information Services on your computer, see Unable to create socket on port 21, for instructions resolving IP conflicts with EFT Server.

Port conflicts

When you create more than one site, each site needs its own port, the place where it listens for user connections and commands. The port for a site is often described as the data channel.

When you are running multiple sites, check your site settings to insure that each site has its own port. When two sites are both assigned the same port, you may have a port conflict. Only one site will be able to run at a time.

FTP sites

The default port for FTP sites is 21, but you can select any number between 1 and 65,535.

> **Note:**
> Assigning a port number under 1024 (other than 21) may lead to conflicts with other programs running on your computer.

Unable to create socket on port 21

The following error is generally the result of running the Microsoft IIS FTP server and the EFT Server on the same computer.

By default the FTP server in Microsoft IIS binds to port 21 on any and all IP addresses. If you want to run both the IIS FTP server and Enhanced File Transfer Server, you will need to disable socket pooling for the IIS FTP server.

To disable socket pooling in IIS FTP server

1. In Microsoft Internet Information Services, stop the FTP site (see below).
2. Open a command prompt window (see below).
3. Change directories to **C:\InetPub\Adminscripts.**
4. Type **CSCRIPT ADSUTIL.VBS SET MSFTPSVC/DisableSocketPooling TRUE** and press the **Enter** key. You should get a response like this;

disablesocketpooling : (BOOLEAN) True

4. Exit the command prompt and restart the FTP site. This should prevent IIS from binding to all IP addresses on port 21, freeing up an IP address for CuteFTP on the default FTP port of 21.

More information on Microsoft IIS socket pooling is available at:

http://support.microsoft.com/default.aspx?scid=kb;en-us;259349

http://support.microsoft.com/default.aspx?scid=kb;EN-US;238131

These links discuss the IIS Web server, but the same information applies to the IIS FTP server.

To open a command prompt window and change directories

1. On the Windows task bar, choose **Start > Run**.
2. Type **cmd** and click **OK**. The command prompt window opens.
3. Type **cd InetPub\AdminScripts** and press the **Enter** key on your keyboard.
4. You should now see **C:\InetPub\Adminscripts>**.

To stop and start an IIS FTP site

1. On the windows desktop, right click **My Computer** and choose **Manage**. The **Computer Management** window opens.
2. In the left pane, select **Services and Applications**.

3. In the right pane, double-click the **Internet Information Services** folder. New items appear in the right pane.
4. In the right pane, select **Default FTP site**.
5. On the menu bar, choose **Action > Stop** to stop the FTP site, or choose **Action > Start** to start the FTP site.

FTP client hangs on the list command

Internet Security and Acceleration (ISA) Server maintains secondary connections for secure network address translation (NAT) clients in Kernel mode, which can improve data throughput for protocols that use secondary connections. Secondary connections for secure NAT clients are only supported if an application filter that can process the protocol is installed on ISA Server.

For example, File Transfer Protocol (FTP) uses the secondary connection over port 20 to transfer data. Because the primary connection is enabled only if the requirements for all applicable rules are met, and the secondary connection is established only after the primary connection is established, there is no need to inspect the traffic for this connection.

For more information on correcting this problem, view the following articles in Microsoft's knowledge base:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q279347

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q294679

Files/Folders do not show the date and time modified, only the year

When a file or folder was last modified in the same year as the server current time, the HOURS:MINUTES display in the directory listing. However, if it was last modified during a previous year, it only displays the YEAR modified.

This is not a bug, it is standard directory listing behavior for Unix systems. For example, if you look at the sites pre-built into CuteFTP Professional, you will notice that this type of folder/file listing is typical for many FTP servers. Additionally, this listing behavior is standard for Redhat Linux, Macintosh operating system support, Microsoft and Palm.

Users have to wait a long time before they can resume an upload

If users frequently lose their connection to Enhanced File Transfer Server, resuming an upload may take several minutes.

If you want to allow users with problematic connections to quickly resume broken uploads, you will need to set their accounts to time out quickly.

If users lose their connection to EFT Server while uploading a file, the portion of the file on the server will remain locked to changes (like a resumed upload) until the server tries to

disconnect. Generally, EFT Server will not try to disconnect until nothing has happened for the amount of time set in **Enable time out**.

The default connection time out value in **Enable time out** is 600 seconds (ten minutes). It can be set as low and 1 second, and as high as 9999 seconds (almost 3 hours), but a connection time out at 30 seconds or 60 seconds will be less likely to interfere with transfer tasks.

When you set the time out value, you can tell the users the value, and if they have an FTP client that automatically attempts to reconnect and resume the transfer, they can set their client to wait the same amount of time before reconnecting.

To set accounts to time out quickly

1. In EFT Administrator, select the **Server** tab. You should be connected to the server.
2. Select the User or User Setting Level you want to configure from the left-hand navigation tree.
3. Select the **Quota** tab from the right-hand pane.
4. Select **Enable time out** and enter the maximum allowable seconds of inactivity allowed before the user is disconnected. If the check box is gray or blank, click until you see a black check in a white box. See Inheritance for more information.
5. Select **Apply**.

Resetting the administrator password

If you cannot remember your password to log in to the administration interface, you will need to reset the password. Resetting the administrator username and password using this procedure will result in the loss of all user and group specific settings. The user accounts and their folder structures will remain, but permissions and settings will be lost.

To reset the administrator username and password

1. In the Windows **Control Panel**, choose **Administrative Tools > Services** and stop the EFT Server service.
2. Navigate to the folder where Enhanced File Transfer Server is installed. By default this will be **C:\Program Files\GlobalSCAPE\EFT Server.**
3. The user accounts and folder structures are stored in one or more of the files containing a **.aud** extension. Copy these configuration files to a safe place for backup.
4. Using the Windows **Add/Remove Programs** utility, uninstall EFT Server.
5. Reinstall EFT Server entering a new administrator username and password. If you need to download the software you can do so from here ftp://ftp.globalscape.com/pub/
6. Start the software and login through the administrator interface with a new username and password.

7. Recreate your FTP site(s) with the EXACT same site name as what was previously used. The site name must match character for character.
8. In the Windows **Control Panel**, go to **Administrative Tools > Services** and stop the EFT Server service.
9. Navigate to the folder containing the **.aud** files from Step three above and copy the files back into the folder where you have installed EFT Server. Choose **Yes** when asked if you want to overwrite the existing **.aud** files.
10. Restart EFT Server and log in. The individual groups and user accounts should be preserved. You must reassign permissions and settings.

Site settings are lost when the service is stopped

If you lose settings and user accounts whenever you restart the EFT Server service, you need to reset permissions on the computer where the Server service is running.

The service runs under a user account. That account must have full administrative rights to the folder where you installed EFT Server. With administrative rights the service can save all your settings.

Server service will not start

If you get an error similar to "Could not start the EFT Server service on Local Computer..." there may be a minor problem in your registry.

To start the EFT Server service

1. On the computer where EFT Server is installed, select **Start>Run**.
2. The **Run** dialog appears. In **Open**, enter **regedit**. The **Registry Editor** window appears.
3. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EFT Server**
4. Select **ImagePath**.
5. On the **Registry Editor** menu bar, choose **Edit > Modify**. An **Edit String** window appears.
6. Add quote marks before and after the text in the **Value Data** box. When you have placed the quote marks it should look similar to this: **"C:\Program Files\GlobalSCAPE\EFT Server\cftpstes.exe"**.
7. Select **OK**. The **Edit String** window closes.
8. Close the **Registry Editor**. EFT Server should restart.

Connecting with Microsoft Internet Explorer

A connection to EFT Server using Microsoft's Internet Explorer (MSIE) can normally be accomplished using the default settings for both products. You may need to allow two or more concurrent connections from the same user and the same IP address to facilitate connection from a Web browser.

For your convenience, some basic connection and troubleshooting information is shown here. If you continue to have trouble establishing a connection using MSIE, you should consult the MSIE documentation or help file.

Depending on the firewall configuration on either the FTP client or server side, you may need to change the mode that is used by the FTP client. MSIE 5 and later support both Standard (PORT) and Passive (PASV) modes.

To Change the MSIE FTP Client Mode

1. Start Internet Explorer.
2. On the **Tools** menu, select **Internet Options**.
3. Select the **Advanced** tab.
4. Under **Browsing**, clear **Enable folder view for FTP sites**.
5. Select **Use Passive FTP (for firewall and DSL modem compatibility)**.
6. Select **OK**.

If you select the **Enable folder view for FTP sites**, MSIE behaves as a Standard (PORT) mode FTP client even if you also select **Use Passive FTP**. If you clear the **Enable folder view for FTP sites** check box and then select the **Use Passive FTP** check box, MSIE behaves as a Passive (PASV) mode FTP client. By default, both MSIE and EFT Server use Standard or Port mode.

Standard (PORT) mode FTP clients first establish a connection to TCP port 21 on the FTP server. This connection establishes the FTP command channel. The client sends a PORT command over the FTP command channel when the FTP client needs to receive data, such as a folder list or file. The PORT command contains information about which port the FTP client receives the data on. In Standard (PORT) mode, the FTP server always sends data from TCP port 20. The FTP server must open a new connection to the client when it sends data.

Passive (PASV) mode FTP clients also start by establishing a connection to TCP port 21 on the FTP server to create the control channel. When the client sends a PASV command over the command channel, the FTP server opens an ephemeral port (between 1024 and 5000) and informs the FTP client to request data transfer from that port. The FTP server responds to the request by using the ephemeral port as the source port for data transfer. If this occurs, the FTP server does not have to establish a new inbound connection to the FTP client.

Firewall configuration

Many firewalls do not accept new connections through an external interface. The firewall may detect these connections as unsolicited connection attempts and, therefore, drop them. Standard mode FTP clients do not work in this environment because the FTP server must make a new connection request to the FTP client.

Firewall administrators may sometimes not want to use Passive (PASV) mode FTP servers because the FTP server can open any ephemeral port number. Although EFT Server by default uses the default ephemeral port range of 1024 through 5000, many FTP servers are configured with an ephemeral port range of 1024 through 65535. Firewall configurations that allow full access to all ephemeral ports for unsolicited connections may sometimes be considered unsecured.

Internet Explorer warning on Windows 2003

When you first install and start EFT Server, you may see an Internet Explorer Warning about security. Select **Add** to allow Internet Explorer to recognize content from www.globalscape.com as safe content.

The message appears because your Internet Explorer settings are set at **High Security**. The trial version of EFT Server attempts to open a page from the Internet to update you on the status of the trial.

After you register the full version of EFT Server, you can change your Internet Explorer security settings and remove globalscape.com from your list of trusted sites.

This issue occurs most often in new installations of Windows 2003 Server.

The system could not find the environment option that was entered

If your EFT Server service will not start and it generates this error message: "The system could not find the environment option that was entered", then make sure:

- The system account the Server service runs under has full access to the Server executable (cftpses.exe).
- You are launching the service from the NT Services applet, not from the command prompt.

Server will not run on Windows XP

Some versions of Windows XP have an built-in Internet Firewall that blocks FTP traffic. This firewall is active by default.

To turn off the Windows XP firewall

Follow the instructions Microsoft has posted on their Web site at http://www.microsoft.com/WINDOWSXP/home/using/howto/homenet/icf.asp.

Changing the log file format kicks users off the server

Any active users are kicked off the server whenever the log file format is changed. It is recommended that the log file format is selected as part of the initial configuration before you start any sites.

System cannot find the environment option that was entered

If Enhanced File Transfer Server will not run and generates the error message "The system could not find the environment option that was entered," verify that the system has full access to the EFT Server executable (cftpses.exe). Also, make sure you are launching the service from the NT Services applet, not from the command prompt.

16

Index