## Post Transfer Actions

Configure PTAs in Gateway Administrator 39
  Define a PTA in Gateway Administrator 41
  Add a PTA to a Transfer Site 44
Configure PTAs in Reflection for Secure IT 44
  Define a PTA in Reflection for Secure IT 45

## Gateway Administrator User Interface

Transfer Sites 48
  Transfer Site Configuration 49
Users 52
  New User 52
  Edit User 53
Groups 54
  New Group 54
  Edit Group 55
  Add Members 56
Actions 56
  Action Configuration 57
System 57
  LDAP Servers Tab 58
  LDAP Server Configuration 58
  Email Server Tab 60
  Email Templates Tab 61
  File Storage Tab 62
  Authentication Tab 63
  PKI Servers Tab 64
  PKI Server Configuration 64

## FileXpress Gateway System Administration

Configuration Email Messages in FileXpress Gateway 67
  Initial Email Setup 67
  Email Notifications 67
  Customize Email Templates 68
  Email Tokens 70
### Configuring the File Storage Server
- Configure File Storage on the FileXpress Proxy 73
- Configure File Storage on an SFTP Server 74
- Configure Additional SFTP Servers Using the FileXpress Secure Shell Proxy 74

### Server Certificate Management
- Replace the Default Server Certificate 77
- Configure Your Browser to Trust a Self-Signed Certificate 80
- Using the Keytool Utility to Manage Keystores 82

### Configuration and Data Files
- Gateway Administrator Properties File 88
- FileXpress Transfer Server Properties File 90
- FileXpress Gateway Data Files 91
- Backing Up Gateway Administrator Data 93

### Managing the FileXpress Gateway Services
- Start and Stop the FileXpress Gateway Administrator Service 94
- Start and Stop the FileXpress Transfer Server 94
- Start and Stop the FileXpress Secure Shell Proxy 95
- Change the Privileges of the Gateway Administrator Service 95
- Reset the Gateway Administrator to All Defaults 96
- Change the FileXpress User Access Account on the FileXpress Secure Shell Proxy 97

### Ensuring High Availability of the FileXpress Gateway Servers
- Create a Gateway Administrator Cluster 99
- Configure Gateway Administrator for Failover and Load Balancing 102
- Remove a Server from a Gateway Administrator Cluster 103
- ConfigServer Command Line Utility 104
- Configure Multiple FileXpress Proxy Servers 105

### Set Up File Transfer Auditing 108

### Change the JRE 109

### Customize the Look of the Transfer Client Web Pages 111
Introduction

FileXpress Gateway provides a secure way to manage file exchange. Secure authentication and encryption are used for all connections. Two possible configurations are shown below.

The simplest configuration has only two components. All FileXpress Gateway services are located on a single server, and files are transferred to and from this server. This configuration can be helpful for initial testing even if your final plans involve a more complex configuration.

A typical distributed configuration is shown below. This configuration supports secure file exchange with users outside your network. Files are transferred through a proxy in the DMZ to a file storage server behind the firewall. In this configuration, the FileXpress Gateway Administrator (which manages user and transfer configuration) also runs securely in the internal network.

- **User workstation**
  Users log on to the web-based FileXpress Secure Shell Proxy Transfer Client using an email link or a URL you provide. It provides an easy drag-and-drop interface for transferring files.

- **FileXpress Gateway Proxy**
  In all configurations, the FileXpress Gateway Proxy runs the following two services:
  - FileXpress Transfer Server: Provides the Transfer Client web application and communicates with the FileXpress Gateway Administrator for user authentication and transfer site configuration information.
• FileXpress Secure Shell Proxy: Manages Secure Shell file transfers to and from the designated file storage location.

In the simpler configuration, the FileXpress Gateway Administrator also runs on this system, and files are uploaded and downloaded directly to and from this server.

In the distributed configuration, the FileXpress Gateway Proxy is not used for file storage. Instead, it acts as a gateway to a file server located behind the firewall. With this configuration, data streams continuously through the gateway, eliminating the need to save files on this server. This is more secure and more efficient than file transfer solutions that require the file to be stored and then forwarded.

▪ FileXpress Gateway Administrator

The Gateway Administrator service maintains user and transfer data and provides a web-based tool for provisioning users and configuring transfers. You can use it to provide access to external users (such as customers or business partners), as well as to allow access to remote employees (users with domain accounts in Active Directory who are working outside your firewall).

▪ File storage

In the simplest configuration, you upload and download files to and from the FileXpress Gateway Proxy. However, in most cases you will want to store files securely behind your firewall. You can configure FileXpress to transfer files to and from a designated file storage server. This can be a Windows system running the Reflection for Secure IT server (included with FileXpress Gateway) or any other SFTP-enabled SSH server.
Installation and System Requirements

In this Chapter

- Server System Requirements 10
- Transfer Client Requirements 11
- Installing FileXpress Gateway 11
- Ports and Firewall Configuration 13

Server System Requirements

FileXpress Gateway is supported on the following platforms:

- Windows Server 2012 R2 on Intel or equivalent, 64-bit
- Windows Server 2012 on Intel or equivalent, 64-bit
- Windows Server 2008 R2 on Intel or equivalent, 64-bit
- Windows Server 2008 on Intel or equivalent, 64-bit
- VMWare vSphere Hypervisor (ESXi) running supported platforms

FileXpress Gateway Administrator Web Application

The FileXpress Gateway Administrator provides a web-based application that you can run directly from the computer on which you have installed the FileXpress Gateway Administrator service, or from any system with access to this computer. It has been tested on the following web browsers. JavaScript and cookies must be enabled.

- Microsoft Internet Explorer (version 9 or later, Windows only)
- Mozilla Firefox
- Google Chrome
- Apple Safari (version 6.1 or later, Mac only)

PKI Services Manager

If your client users will authenticate using X.509 certificates or Smart Cards, you need to install and configure Reflection PKI Services Manager, which is available at no additional charge from the FileXpress Gateway download page.

- Reflection PKI Services Manager version 1.3 or later
Note: For additional recommendations to help ensure a secure environment, see Security Recommendations for the FileXpress Gateway Proxy (page 21).

Transfer Client Requirements

The FileXpress Transfer Client is a Java applet that runs in a web browser. Client workstations must meet the following requirements.

- Users must be running one of the following supported browsers. JavaScript and cookies must be enabled.
  - Microsoft Internet Explorer (version 9 or later, Windows only)
  - Mozilla Firefox
  - Google Chrome
  - Apple Safari (version 6.1 or later, Mac only)
- Java must be installed.
  - Users who don't have Java installed will see a message with information about how to download Java when they first try to connect. Java is available free of charge from the Oracle website: http://java.com/en/download/

Connections from other Secure Shell Clients

This guide describes how to manage transfers from user workstations using the FileXpress Gateway Transfer Client, but using this client is not a requirement. FileXpress users can also use the Reflection for Secure IT Secure Shell client, the Reflection FTP Client configured for SFTP transfer, or any other SFTP-enabled SSH client.

Installing FileXpress Gateway

Before you install FileXpress Gateway, review the configuration options described in the Introduction (page 8).

- For the simplest configuration, you can install all FileXpress Gateway services on a single system. (The optional Reflection for Secure IT Server cannot be installed on this system.)
- For a distributed configuration, you will need to run the installer on each computer in your configuration, selecting the appropriate features for each installation, as described in the procedure below.

Note: You must install the same version (and build) of all FileXpress Gateway components.
To install FileXpress Gateway

1. Log on to Windows using an Administrator account.

2. Start the Setup program (setup.exe).

   When you download FileXpress Gateway from the Attachmate download site, you are first prompted to select a folder in which to extract the installation files. This is a temporary location. After this step is complete, the Setup program starts automatically.

3. FileXpress Gateway requires the Microsoft Visual C++ Redistributable Package. It is installed by the Setup program if it is not already on your system. If you see a message saying that this package must be installed, click Continue to install this required software. The FileXpress Gateway installation continues after this prerequisite is installed.

4. Review and accept the license agreement.

5. (Optional) Enter your user information on the User Information tab.

6. Click the Feature Selection tab. Use the table below to determine which features you need to install on each computer in your configuration.

   To remove a feature, click the icon next to the feature name and select Feature will be unavailable. To add a feature, click the icon and select Feature will be installed on local hard drive.

   Note the following:

   • The FileXpress Gateway Proxy and FileXpress Gateway Administrator are both installed by default. This configuration is useful for evaluation and initial testing.

   • The FileXpress Gateway Proxy feature always installs both the FileXpress Transfer Server and the FileXpress Secure Shell Proxy. These two services must always be installed together on the same server.

   • The Reflection for Secure IT Server cannot be installed on the same system as the FileXpress Secure Shell Proxy.

<table>
<thead>
<tr>
<th>Computer you are setting up</th>
<th>Feature(s) to install</th>
</tr>
</thead>
</table>
| A single system that will run all FileXpress Gateway services | FileXpress Gateway Proxy  
                        | FileXpress Gateway Administrator |
| FileXpress Gateway Proxy (Typically runs in the DMZ.) | FileXpress Gateway Proxy |
| FileXpress Gateway Administrator (Typically runs behind the firewall.) | FileXpress Gateway Administrator |
| File storage server (This optional server typically runs behind the firewall.) | Reflection for Secure IT Server |

7. (Optional) To change the default installation folder, click the File Location tab.

8. Click Install Now.

9. On the final installation screen, select Restart my computer for me and click Close.
Installation and System Requirements

Note: The system restart is required to complete the installation.

To confirm that the installed services are running

The FileXpress services are configured to start automatically when you restart Windows. You can use the Windows Services console to confirm that your services are running.

1. Open the Windows Services console (Start > All Programs > Administrative Tools > Services).

2. Confirm that the services are running. The following services are installed with FileXpress Gateway features:

<table>
<thead>
<tr>
<th>Installed feature</th>
<th>FileXpress service name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileXpress Gateway Proxy</td>
<td>Attachmate FileXpress Transfer Server</td>
</tr>
<tr>
<td></td>
<td>Attachmate FileXpress Secure Shell Proxy</td>
</tr>
<tr>
<td>FileXpress Gateway Administrator</td>
<td>Attachmate FileXpress Gateway Administrator</td>
</tr>
<tr>
<td>Reflection for Secure IT Server</td>
<td>Attachmate Reflection for Secure IT Server</td>
</tr>
</tbody>
</table>

Note: After these services are started by a Windows system restart or by using the Services console, it might take a few minutes before they are available for use.

Ports and Firewall Configuration

The following default ports are used in a distributed FileXpress Gateway configuration.

<table>
<thead>
<tr>
<th>Port</th>
<th>Connection Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>From external clients to the FileXpress Secure Shell Proxy for SFTP connections.</td>
</tr>
<tr>
<td></td>
<td>From the FileXpress Gateway Proxy to the SFTP file storage server for SFTP connections.</td>
</tr>
<tr>
<td>9492</td>
<td>From external clients to the FileXpress Transfer Server for HTTPS connections.</td>
</tr>
<tr>
<td>9190</td>
<td>From the FileXpress Gateway Proxy to the FileXpress Gateway Administrator for web service calls.</td>
</tr>
<tr>
<td>9490</td>
<td>(optional) From the FileXpress Gateway Proxy to the FileXpress Gateway Administrator.</td>
</tr>
<tr>
<td></td>
<td>Opening this port is only required if you want to launch FileXpress Gateway Administrator from the FileXpress Secure Shell Proxy console running in the DMZ.</td>
</tr>
</tbody>
</table>
Note: If you configure multiple instances of Gateway Administrator to support clustering (page 99), additional ports must be open between the Gateway Administrator instances. These ports support cluster configuration (43000 by default) and data replication (8846 by default).
**Enable FileXpress Connections in the FileXpress Secure Shell Proxy**

To support file exchange using the FileXpress Gateway, you must configure the FileXpress Secure Shell Proxy to enable access by FileXpress users.

**Before you begin**

- Install the FileXpress Gateway Proxy services and the FileXpress Gateway Administrator (page 11).

**To enable FileXpress Gateway transfers**

1. Start the FileXpress Secure Shell Proxy console. It is installed in the Windows Start menu (or Apps list) under *Attachmate FileXpress Gateway > FileXpress Secure Shell Proxy*.

2. On the *FileXpress Users* pane, enable *Allow access to FileXpress users*.

3. For *Gateway Administrator host*, enter the name or IP address of the computer running the FileXpress Gateway Administrator. (If you installed all FileXpress Gateway services on the same computer, you can leave the default value, localhost.) Leave the default port value (9190). FileXpress Gateway Administrator is configured to listen on this port by default.

4. Click *Activate and verify*. This saves your settings and triggers actions that ensure that the FileXpress Proxy services can establish a secure connection with the Gateway Administrator.

   - You will be prompted to accept the certificate presented by the Gateway Administrator server. Click *Yes* to establish the trust relationship.
When the configuration update is complete, click **Close** to close the **Web service connection** dialog box.

Click **Yes** when prompted to restart the FileXpress Transfer Server service. This step is required.

---

**Note:** By default, **FileXpress user access account** is set to **Service account**. With this setting FileXpress users run using the same privileges as the FileXpress Proxy Secure Shell Proxy service (the Local System account). You can also specify an alternate user account with more limited privileges. For details, see Change the FileXpress User Access Account on the FileXpress Secure Shell Proxy (page 97).

---

**Initial Logon to the FileXpress Gateway Administrator**

FileXpress Gateway Administrator is a web-based tool for provisioning users and configuring transfers. Use this procedure to connect to Gateway Administrator and log on. Your initial logon resets the default administrative password.

---

**Before you begin**

Install the FileXpress Gateway Administrator (page 11).

---

**To connect to the FileXpress Gateway Administrator and log on**

1. Connect to the FileXpress Gateway Administrator console using either of the following methods:

   On the server running FileXpress Gateway Administrator, use the Windows Start menu (or Apps list). It is installed under **Attachmate FileXpress Gateway > FileXpress Gateway Administrator**.

   - **or**-

   From a web browser on any system with access to the FileXpress Gateway Administrator server, enter the following URL replacing `<gateway_administrator_host>` with the name or IP address of the host running FileXpress Gateway Administrator.

   ```
   https://<gateway_administrator_host>:9490
   ```

   **Note:** You will see a warning message before you see the login page. This warning shows up because the FileXpress Gateway Administrator installs with a self-signed security certificate that is unknown to your browser. For initial testing purposes, you can ignore this warning and proceed with the connection (Internet Explorer or Chrome) or add an exception (Firefox). For more information, see Server Certificate Management (page 77).

2. For your initial logon, enter the following credentials:

   **Username:** admin

   **Password:** secret
Immediately after your first logon, you will be prompted to change the password for the admin account.

Note: If you are configuring Gateway Administrator in a production environment, use a secure password that meets your company’s password requirements.

Use the next procedure to specify an actual email address for the default admin user.

To update the email address of the default admin account

1. From Gateway Administrator, click the Users tab.
2. Select the default "admin" user and click Edit.
3. Edit Email address and click Save.

Note: After you begin to provision actual users, you should add appropriate users to the Administrators group to replace the default admin account. This helps ensure that the correct users will have full access to FileXpress Gateway configuration, and that backup administrators are available to provide access if needed. For details about how to add Windows domain users to the Administrators group, see Add LDAP Users to the Administrators Group (page 28).

Configure Email Support in FileXpress Gateway Administrator

FileXpress supports a number of optional email notification services. These include:

- Account creation email for new users
- Password reset email
- Transfer site access notifications
- Notifications sent to site managers and/or site members when files are uploaded or downloaded

To support these services, you need to configure access to an email server and configure the server address that will be used in URL links included in email messages.

To configure the email server connection

1. Log on to Gateway Administrator using the default admin account (or any account that has the System setup role enabled).
2. Go to System > Email Server.

   • Set Email service to Enabled. This step is required to make the remaining items editable.
   • For SMTP server, enter your email server name or IP address.
   • Configure additional options appropriate for your mail server. For details, see Email Server Tab (page 60).
• If **Check server identity** is selected (recommended), click **Retrieve Certificate**.

3 Click **Test Connection**. (This tests the current on-screen settings. These settings are not saved until you click **Save**.)

4 Click **Save**.

The connection test on the **Email Server** page confirms that the server can be reached, but does not confirm that outgoing messages will be successful. You can use the next procedure to test an outgoing email. This helps ensure that the email server settings you entered meet your email server’s requirements.

**To test an outgoing message using your email server settings**

1 Click the **Email Templates** tab. The Account Creation template is displayed by default.

2 Below the template text, click **Preview** to expand this portion of the page.

3 Enter your email address in the **To** box.

4 Click **Send Test Email**. You should receive a sample Account Creation email.

Emails sent to FileXpress users include a URL that they can use to initiate a password reset or connect to the FileXpress Transfer Client. By default, these links use "localhost" as the server name. To enable Gateway Administrator to create links that connect correctly to the Transfer Server, you need to change this default by editing the Gateway Administrator properties file (page 88), as described in the next procedure.

**To configure the base server URL used in email message links**

1 Open the **Gateway Administrator** `container.properties` in a text editor. The default location of this file is:
   
   C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\conf\container.properties

2 Locate the following lines:

   ```
   # Public facing base URL of Transfer Server (for example https://attachmate.com:9492)
   transfer.server.url=https://localhost:9492
   ```

3 Replace `localhost` with the host address of your FileXpress Transfer Server. For example:

   ```
   transfer.server.url=https://myhost.filexpress.com:9492
   ```

4 Save the edited properties file.

5 Restart the Attachmate FileXpress Gateway Administrator service (page 94). A restart is required after any changes to the properties file.

---

**Set Up the File Storage Server**

FileXpress transfer sites use directories on a designated file storage server for file upload and download. If you are a member of the Administrators group (or have the **System setup** role enabled), you can use Gateway Administrator to designate which server should be used for file storage.
File storage on the FileXpress Gateway Proxy

By default, Gateway Administrator is configured to use the FileXpress Proxy server for file storage. This configuration is appropriate for initial testing, or if you use the FileXpress Proxy to manage transfers within your internal network. You do not need to modify any default settings to use this configuration.

For information about customizing the directory used for file storage on the FileXpress Proxy, see Configure File Storage on the FileXpress Proxy (page 73).

File storage on a back end SFTP server

If you run the FileXpress Proxy in the DMZ, you can configure FileXpress Gateway to store files securely behind your firewall, as shown below. In this configuration, data streams continuously through the FileXpress Proxy, eliminating the need to save data on the FileXpress Proxy.

For information about setting up a back end file storage server, see Configure File Storage on an SFTP Server (page 74).

Use Quick Add to Add a Transfer Site and New User

The Quick Add feature adds a user and transfer site in one simple step. You can use this procedure to confirm that email registration is working and that users can successfully transfer files.

Before you begin

- Configure Email support in FileXpress Gateway Administrator (page 17).

To create a user and transfer site

1. Log on to Gateway Administrator using the default admin account (or any account that has the Manage transfer sites and Manage FileXpress users roles enabled).
2. On the Transfer Sites page, click Quick Add.
3 Enter a **Transfer site name**.

---

Note: Site names must be unique. If you enter an existing name, you will see an error message when you click **Create**.

---

4 Enter a **User email address**. For initial testing, use an account that you have access to.

---

Note: Each email address is associated with a unique user. When you specify an email address that does not yet exist in the database, the new user will be created with the email address as the UserID. If you enter an existing email, the new transfer site is added and made available to that user. The email registration steps below assume that this is a new email.

---

5 Click **Create**.

6 When the email address is not associated with an existing user, you will see a confirmation prompt asking if you are sure you want to create a new account. Click **OK** to confirm.

If you don't see a confirmation prompt, it means that a user account with this email already exists.

---

**To complete user registration and log on to the Transfer Client**

1 Log on to the email account you specified for the new user. You should see two email message sent from FileXpress Gateway. If you have made no changes to the default email templates, the subject lines say "Your FileXpress user account" and "FileXpress File Sharing: You Have Access to a Transfer Site."

2 Open the email with the subject line "Your FileXpress user account."
   - Note that the username for the account you just created is your email address.
   - Look at the link in this email and confirm that the URL is correct for your FileXpress Transfer Server. If the host name in the URL is "localhost," see Configure Email Support in FileXpress Gateway Administrator (page 17).

3 Click the link or copy it into your browser.

   Your browser displays a warning message. This is because the FileXpress Transfer Server installs with a self-signed security certificate that is unknown to your browser. For initial testing purposes, you can ignore this warning and proceed with the connection (Internet Explorer or Chrome) or add an exception (Firefox). After you replace the self-signed certificate with one signed by a well-known Certificate Authority, users won't see this warning. For more information, see Server Certificate Management (page 77).

4 You will see a password reset page. In the **Username** box, enter your email address and click **Reset**.

   You will see a message saying the instructions for creating a password have been sent to your email address.

5 Return to your email account to find the FileXpress password request message. Click the link in this message to go to the **Change password** page.

6 Enter your username, set your password, and click **Submit**. This action submits your new password and connects you to the Transfer Client.
You will see additional warning messages. Java uses security messages to ensure that only software you approve runs on your system. For each message, confirm that you want to continue. For more information about these messages and how to turn off their display, see Connect to the Transfer Client (page 36).

7 After a successful login to the Transfer Client (page 37), you can test the transfer site using drag-and-drop to upload a file.

8 Return to your email account to confirm that you received a FileXpress account update email message.

**Configure Server Certificates**

When you log on to Gateway Administrator, the browser connects to the FileXpress Gateway Administrator server. When users log on to the Transfer Client, the browser connects to the FileXpress Transfer server. In both cases, the connection is made using HTTPS and the default configuration results in certificate warning messages.

**Why you see certificate warning messages**

When an HTTPS connection is established, the browser requires server authentication. By default, the FileXpress Gateway servers send a self-signed security certificate to the browser for this purpose. (A self-signed certificate is signed by the same entity that it certifies.) The browser checks the digital signature in this certificate against its list of trusted Certificate Authorities (CAs). You see a certificate warning because the signer of the certificate is not in your browser's list of trusted CAs.

**Managing certificates**

Depending on where you are in your FileXpress Gateway evaluation and configuration process, you can use any of the following approaches to manage server certificates.

- Use the default self-signed certificates and ignore the certificate errors.
  This option is appropriate during initial testing.

- Configure your browser to trust the self-signed certificates (page 80).
  This option is appropriate during initial testing. You might also choose this as a permanent option for the Gateway Administrator.

- Replace the server's self-signed certificate with a certificate from a well-known Certificate Authority (page 77).
  Make this change to the FileXpress Transfer Server before you provide end users with URLs for launching the Transfer Client. This change enables Transfer Client users to connect securely without seeing certificate warning messages.

**Security Recommendations for the FileXpress Gateway Proxy**

Use the following precautions to help ensure security on the FileXpress Proxy (the system running the FileXpress Secure Shell Proxy and the FileXpress Transfer Server).

- Do not join the server to a Windows domain.
Do not run non-essential services on the server that might provide user access, such as Telnet servers, FTP servers, and SQL servers.

In the FileXpress SSH Proxy Server console:

- On the **FileXpress Users** pane, leave **Allow server access to FileXpress users only** and **Restrict FileXpress users to file transfer sessions** selected. These default settings help minimize external user access to your system.

- Change the user access account (page 97) to an account with more limited privileges than the default service account.

- Disable port forwarding for all users. To do this, clear both port forwarding options on the **Permissions** pane under **Tunneling**.

- Configure firewalls (page 13) that limit access to ports on your servers.
Add Users to the FileXpress Directory

You can add users to Gateway Administrator's built-in FileXpress directory when you want to exchange files securely with users who do not have accounts in your Windows Active Directory. Several methods are available for adding new users.

You can create users with or without creating a transfer site at the same time. This table summarizes the features of each option.

<table>
<thead>
<tr>
<th>Method</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users &gt; New</td>
<td>▪ Add a user without creating a transfer site. Users can be added to transfer sites later.</td>
</tr>
<tr>
<td></td>
<td>▪ Configure both UserID and Email address. These can be the same or different.</td>
</tr>
<tr>
<td></td>
<td>▪ Choose either Email registration or Specify password. If you select Specify password, no email is sent automatically from FileXpress; you must send login credentials to the user.</td>
</tr>
<tr>
<td></td>
<td>▪ Configure group membership when you add the user.</td>
</tr>
<tr>
<td></td>
<td>▪ Required Role: Manage FileXpress users.</td>
</tr>
</tbody>
</table>
Method | Features
--- | ---
**Transfer Sites > Quick Add** |  
- Add a user when a new transfer site is created.  
- UserID is set automatically to the user's email address.  
- User is added with no group membership. Users can be added to groups later.  
- User is given default site permissions. Site permissions can be modified later by editing the transfer site.  
- Required Roles: **Manage FileXpress users** and **Manage transfer sites**.

**Transfer Sites > Add (or Edit)** |  
- Add a user when you create a new transfer site or edit an existing site.  
- UserID is set automatically to the user's email address.  
- User is added with no group membership. Users can be added to groups later.  
- Modify the default site permissions for any user (new or existing).  
- Required Roles: **Manage FileXpress users** and **Manage transfer sites**.

---

**To add a user from the New User page**

1. Connect to Gateway Administrator and log in using an account that is a member of the Transfer Site Administrators group (or any group that has the **Manage FileXpress users** role enabled).
2. On the **Users** tab, click **New**.
3. Enter user information. See New User (page 52) for details. Note the following:
   - To support **Email registration**, email support must be configured (page 67).
   - If you select **Specify password**, no email is sent automatically from FileXpress; you must send login credentials to the user.
   - Group membership is optional. All FileXpress users can log on to the FileXpress Transfer Client, and transfer site access can be configured for individual users or groups.
4. Click **Save**.

**Delete or Disable Users**

You can permanently delete a FileXpress user or disable an account without removing it from the database.

---

Note: LDAP user accounts must be managed on the LDAP server.
To delete a FileXpress user

1. Connect to Gateway Administrator and log in using an account that is a member of the Transfer Site Administrators group (or any group that has the Manage FileXpress users role enabled).

2. On the Users tab, select the user and click Delete. You will be prompted to confirm this action.

To disable a FileXpress user

1. Connect to Gateway Administrator and log in using an account that is a member of the Transfer Site Administrators group (or any group that has the Manage FileXpress users role enabled).

2. On the Users tab, select the user and click Edit.

3. Set Account expires to a date in the past. (To enable an expired account, set this to a date in the future.)

Add Users from an LDAP Server

Use the LDAP Servers tab to add users to FileXpress Gateway who have accounts in Windows Active Directory. You can use this approach to provide transfer site access to Windows domain users who are working remotely. Authentication and group membership are managed on the LDAP server. Each time the user logs in, current information is retrieved from the LDAP server.

To configure LDAP servers, you must be a member of the Administrators group, or any group with System setup enabled.

To add users from an LDAP server

1. Log on to Gateway Administrator using an account in the Administrators group (or any account that has the System setup role enabled).

2. Go to System > LDAP Servers.

3. Click New.

4. Enter information for connecting to your LDAP server. For details, see LDAP Server Configuration (page 58).

   Note that the value for UserID must include the domain. For example:

   mydomain\user

   -or-

   user@mydomain

5. Click Test Connection to confirm that Gateway Administrator can access your LDAP server. This test verifies the connection, but does not save your settings.

6. Click Save.

You can view users and groups that are brought in from an LDAP server, but cannot modify them. These users and groups must be managed on the LDAP server.
To view LDAP users and groups

1. Click the Users or Groups tab.
2. Use the LDAP server drop-down list to select your LDAP server. (If you don't see your server in the list, return to the LDAP configuration page and confirm that you saved your settings.)

Creating and Editing Groups

You can create and edit groups in the FileXpress directory. You cannot modify the groups in added LDAP servers; however, you can add users from an added LDAP server to your FileXpress groups.

There are two ways to change FileXpress group membership.

- Edit a group
  You can add or delete members from any existing group. If you are creating a new group, you need to create the group first, then modify the members list as a separate step.

  This option allows you to add members of the FileXpress directory and any added LDAP servers.

  Required role: System setup

- Edit a user
  You can modify the list of groups that a user is a member of.

  This option is available only for members of the FileXpress directory.

  Required roles: System setup and Manage FileXpress users

To add a new group

2. Click New.
3. Enter a GroupID and Description.
4. (Optional) Assign roles (page 27) to this group.
5. Click Save.

To edit a group’s list of members

1. On the Groups page, select a FileXpress group and click Edit.
2. Click Add Members.
3. Set LDAP Server to the directory from which you want to add users.
4. Use Filter User to help you locate the user or users you want to add.
5. Select one or more users and click Add. You can continue adding users in this way.
Note: Clicking **Add** saves the change to the group.

6 When you're done adding users, click **Done**. This closes the **Add Members** page. You should see your added users in the members list.

**To edit a user's group membership**

1 On the **Users** page, select a FileXpress user and click **Edit**.
   • To add a user to a group, use the selection box. Added groups, and the roles the user inherits from these groups, are displayed under the selection box.
   • To remove a user from a group, click the x in the box displaying the group name.
2 Click **Save**.

**Default Groups**

FileXpress Gateway includes two default groups.

- The Administrators group enables members to perform all available actions. The roles in this group cannot be modified and you cannot delete this group.
- The Transfer Site Administrators group enables members to add new users and transfer sites. The roles in this group cannot be modified and you cannot delete this group.

**Roles in FileXpress Gateway**

You can assign roles to any group in the FileXpress directory. To enable users to perform tasks, assign them to a group with the required role or roles enabled.

- To log on to Gateway Administrator, a user must have at least one of these roles enabled.
- To view the roles assigned to a user, select the user in the **Users** list and click **Edit**. See **Roles inherited from group membership** at the bottom of the **Edit User** page.
- The default Administrators group has all roles enabled. In addition, members of this group can view all transfer sites. Only members of this group have this privilege; all other users can view only those sites they have the right to manage.
- The default Transfer Site Administrators group has **Manage transfer sites** and **Manage FileXpress users** enabled.
The following roles are available:

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Setup</td>
<td>Can view Groups, System, and About.</td>
</tr>
<tr>
<td></td>
<td>Can modify all system settings. Can add groups and edit groups and modify the membership list of a group.</td>
</tr>
<tr>
<td>Manage actions</td>
<td>Can view Actions and About.</td>
</tr>
<tr>
<td></td>
<td>Can add and edit Post Transfer Actions.</td>
</tr>
<tr>
<td>Manage transfer sites</td>
<td>Can view Transfer Sites and About.</td>
</tr>
<tr>
<td></td>
<td>Can create and edit transfer sites. Can add existing users and groups to sites. Can add new sites using Quick Add, but cannot provision new users this way. Cannot view the New FileXpress User section of the New Transfer Site page unless Manage FileXpress users is also enabled.</td>
</tr>
<tr>
<td>Manage FileXpress users</td>
<td>Can view Users and About.</td>
</tr>
<tr>
<td></td>
<td>Can add and edit FileXpress users and passwords. Cannot modify group membership.</td>
</tr>
</tbody>
</table>

Add LDAP Users to the Administrators Group

If you have added an LDAP server to FileXpress, you should add users from that server to the FileXpress Gateway Administrators group. This helps ensure that the correct users will have full access to FileXpress Gateway configuration using their Active Directory logon credentials, and that backup administrators are available to provide access if needed.

Note: You might want to retain one or more accounts in the FileXpress LDAP server as members of the Administrators group. This helps ensure that you can log into Gateway Administrator if there is a problem with access to your added LDAP server(s). If you do this, ensure that all FileXpress administrator accounts use a secure password that meets your company's password requirements.

To add LDAP users to the Administrators group

1. Log on to Gateway Administrator using the default admin account (or any account that is a member of the Administrators group).
2. From the Groups page, select the Administrators group and click Edit.
3. Click Add Members.
4. Set LDAP Server to your added LDAP server.
5. Use Filter User to help you locate the user or users you want to add.
6. Select one or more users and click Add. This action saves the change. You can continue adding users in this way.
7. When you're done adding users, click Done. This closes the Add Members page. You should see your added users in the members list.
Click **Done** to exit the **Edit Group** page.

**LDAP Server Advanced Domain Settings**

Users can log into the Transfer Client and Gateway Administrator using just a user ID (for example `joe`) or using a domain name and user ID (`acme\joe`). By default, when a user logs in using just a user ID, FileXpress searches all available LDAP servers for a matching user and authenticates the first matching user it finds; it does not search additional LDAP servers if that fails. When no domain name is included, a UserID for a different domain could match and allow login if the passwords for both accounts are the same.

You can use **Advanced domain settings** on the **New/Edit LDAP Server** (page 58) page to customize how FileXpress manages user authentication to your LDAP server(s). The examples below show how login is handled for some possible configurations.

**Note:** **Advanced domain settings** apply to password authentication only; X.509 certificate authentication always requires user mapping that specifies both a domain and username.

These examples use `acme` as a sample Active Directory domain. For these examples, this `acme` is a domain that requires a valid authentication domain name. It can accept both `acme` and `acme.com` as the authentication domain name.

**Example 1**

Domain Name = `anyName`; Domain Mapping = `anyAlias`; Remove User Domain = **No**, Default Authentication Domain = `none`.

- **Login as **validUser**: Authentication fails because there is no authentication domain name, and this is required by the acme domain.
- **Login as **anyName\validUser or anyAlias\validUser**: Authentication fails because `anyName` and `anyAlias` are not valid authentication domain names.
- **Login as **acme\validUser or `acme.com\validUser`: Authentication succeeds because `acme` and `acme.com` are valid authentication domain names.

**Example 2**

Domain Name = `anyName`; Domain Mapping = `anyAlias`; Remove User Domain = **No**, Default Authentication Domain = `acme`.

- **Login as **validUser**: Authentication succeeds because FileXpress adds the value specified for Default Authentication Domain (`acme`) before authenticating the user.
- **Login as **anyName\validUser or anyAlias\validUser**: Authentication fails because `anyName` and `anyAlias` are not valid authentication domain names.
- **Login as **acme\validUser or `acme.com\validUser`: Authentication succeeds because `acme` and `acme.com` are valid authentication domain names.

**Example 3**

Domain Name = `anyName`; Domain Mapping = `anyAlias`; Remove User Domain = **Yes**, Default Authentication Domain = `none`.
The following results are based on the sample acme domain, which requires a valid domain name for authentication:

- **Login as validUser**: Authentication fails because there is no authentication domain name, and this is required by the acme domain.
- **Login as acme\validUser**: Authentication fails. Although acme is the valid authentication domain name, it is removed before FileXpress attempts authentication.
- **Login as anyAlias\validUser or anyName\validUser**: Authentication fails because authentication is attempted with no authentication domain name.

If your Active Directory domain does not require an authentication domain, the login attempts above will succeed because each of them presents a valid user ID to the domain. In this case, using anyAlias\validUser improves performance because the Domain Mapping directs FileXpress to authentication to this specific LDAP server. Although anyAlias is not the actual domain authentication name, authentication succeeds because the domain name is removed before FileXpress attempts authentication.

### Example 4

This example shows a configuration for handling a merger that brings users from the summit domain into the acme domain. It enables summit users to log in without modifying their familiar credentials.

**Domain Name = acme; Domain Mapping = summit; Remove User Domain= Yes, Default Authentication Domain = acme.**

- **Login as validUser**: Authentication succeeds because FileXpress Gateway uses the value specified for Default Authentication Domain (acme).
- **Login as acme\validUser or summit\validUser**: Authentication succeeds because the entered domain, acme or summit, is removed and default acme is used.
- **Login as anything\validUser**: Authentication succeeds. A domain is provided by the user for which no mappings exist. In this case FileXpress Gateway tries all configured LDAP servers and applies the directory-specific domain rules for each one. Authentication to the acme domain will succeed because the entered domain anything is removed and replaced by acme.

### Configure Certificate User Authentication

By default, users log on to the Transfer Client with a user name and password. You can also configure authentication using X.509 certificates, for example using a Common Access Card (CAC).

---

**Note**: When enabled, certificate authentication applies to all users; it is not possible to configure password authentication for some users and certificate authentication for others.

---

### Before you begin

- PKI Services Manager must be installed, configured, and running, with mapping rules that return a single allowed user for any valid certificate. See Set Up PKI Services Manager (page 32).
You can install and configure PKI Services Manager on multiple systems to ensure availability of certificate authentication services. When you add multiple servers to the PKI Servers list, Gateway Administrator contacts the first available server on the list. The reply from this PKI Server (valid or not valid) is used, and no other servers on the list are contacted. All PKI servers must have identical trust anchors, configuration settings, and mapping files to ensure that each of your PKI Services Manager servers returns the same validation for all certificates.

- Confirm the host name or IP address of the PKI server, and the listening port used by this server (18081 is the default).
- Client workstations must be configured to present certificates for user authentication. This can be done using smart cards or by adding certificates to the browser's personal certificate store.

### Configure Gateway Administrator to contact your PKI Services Manager

1. Log on to Gateway Administrator using an account in the Administrators group (or any account that has the System setup role enabled).
2. On the System tab, click PKI Servers.
3. Click New.
4. For PKI Server, specify the name or IP address of the system running PKI Services Manager (page 32).
5. Click Retrieve Public Key.
   
   If the server is running and available, Gateway Administrator retrieves the public key and displays it. (This key should match the key displayed in the PKI Services Manager console when you go to Utility > View Public Key.)
6. Click Test Connection. If Gateway Administrator can successfully contact PKI Services Manager, you will see a message saying the connection is successful.
7. Click Save. This step is required; verifying the connection does not save the configuration.
   
   You will be returned to the PKI Servers tab with your added server visible in the list.

### Enable Certificate authentication

1. From the Gateway Administrator System tab, click Authentication.
2. Select Client X.509 certificate authentication.
3. Click Save.
   
   After these changes, subsequent user logins to the Transfer Client will not display a user name and password prompt. If a user certificate is available on the client system, Gateway Administrator will send the certificate to PKI Services Manager for validation. If the certificate is valid, PKI Services Manager will use the preconfigured identity mapping to return the name of the user who is authorized to authenticate with the presented certificate.
Set Up PKI Services Manager

Reflection PKI Services Manager is a service that provides certificate validation services. If your client users will authenticate using smart cards or other forms of X.509 certificates, you need to install and configure this service. It is available at no additional charge from the FileXpress Gateway download page. FileXpress Gateway requires version 1.3 or later.

If you installed PKI Services Manager on Windows, you can configure required settings using the PKI Services Manager Console (Start > All Programs > Attachmate Reflection > Utilities). Or, on both Windows and UNIX, you can configure these settings by editing the PKI Services Manager configuration files (pki_config and pki_mapfile). For detailed configuration information, see the PKI Services Manager User Guide, which is available from http://support.attachmate.com/manuals/pki.html.

### PKI Services Manager Configuration

1. Download and install PKI Services Manager.

   PKI Services Manager can run on both Windows and UNIX systems. You can install it on the same system as Gateway Administrator or on another system in your network.

2. Create a certificate store that contains the CA certificates that are required to validate your user certificates. On Windows, you can create a private certificate store or use the Windows certificate store. On UNIX, you need to create a private store (or use an existing store on your system).

3. Specify one or more certificates to act as trust anchors; and specify where PKI Services Manager should search for intermediate certificates when building a path to your trust anchors.

   In the console, use the **Trusted Chain** pane. Or, in pki_config, use the **TrustAnchor** and **CertSearchOrder** keywords.

4. Configure how PKI Services Manager should handle certificate revocation checking.

   In the console, use the **Revocation** pane. Or, in pki_config, use **RevocationCheckOrder**, and (depending on your configuration) **OCSPResponders**, **OCSPCertificate**, and **CRLServers**.

5. Configure how certificates presented by users will map to allowed users. After PKI Services Manager has validated a user certificate, it will use the mapping you configure to return the user name that will be used to log on with this certificate.

   In the console, use the **Identity Mapper** pane. Or, add map rules manually to pki_mapfile.

---

**Note:** For FileXpress Gateway, your mapping configuration must return a single allowed user (including both domain and username) for each certificate. Some sample mapping configurations are shown below.

---

6. Save all settings changes and restart the PKI Services Manager server.
Sample Mapping Rules for Transfer Client Authentication

When users log on to the Transfer Client using certificates, they present the certificate (for example using a CAC card) without entering a user name. The mapping system you devise must use the presented certificate to identify a domain and user (domainName\userName) who can log on to the Transfer Client. The mapping rule must return exactly one user ID. If multiple user ID values are returned, the login will fail.

Note: From the console, you can test mapping rules using Utility > Test Certificate. On UNIX, you can use the pki-client command line utility.

The following examples use a single map rule to return the name of an allowed user based on the contents of the certificate that user presents:

{ %Subject.CN% } The allowed user name is equal to the value of the Subject Common Name field.

{ acme\%UPN.User% } The allowed user name is constructed by combining the domain acme\ with the value found in the userID portion of the UPN field.

It is also possible to configure multiple map rules. PKI Services Manager processes each rule in order until it finds a condition that matches the validated certificate. For example:

RuleType user
{ acme\dgreen } Subject.Email Equals donald.green@acme.com
{ acme\jblue } Subject.Email Equals joseph.blue@acme.com

Rules that return multiple names for the same certificate are not supported for authentication to the FileXpress Transfer Client. The following example returns two valid user names for the same certificate. In this case, a logon attempt using the certificate will always fail.

{ acme\root acme\dgreen } Subject.Email Equals donald.green@acme.com
Managing Transfer Sites

In this Chapter

Connect to FileXpress Gateway Administrator 34
Create a Transfer Site 35
Connect to the Transfer Client 36
The Transfer Client User Interface 37

The procedures in this section are geared to users who are members of the Transfer Site Administrators group. These procedures assume that installation and initial configuration has already been completed by a FileXpress administrator.

Connect to FileXpress Gateway Administrator

FileXpress Gateway Administrator is a web-based application that you can use to manage users and transfer sites. To be able to log onto the Gateway Administrator, you must be a member of the Administrators group, the Transfer Site Administrators group, or any group with at least one of the following roles enabled: System Setup, Manage actions, Manage transfer sites, Manage FileXpress users.

Before you begin

- You need to know the address of the server running FileXpress Gateway Administrator and your login credentials.

To connect to FileXpress Gateway Administrator

- From a web browser, enter the following URL, replacing `<gateway_administrator_host>` with the name or IP address of your server:

  https://<gateway_administrator_host>:9490

Note: You might see a certificate warning message before you see the login page. This warning shows up if the FileXpress Gateway Administrator is still using the default self-signed security certificate that installs with FileXpress Gateway. This message is not displayed if the FileXpress Gateway server has been configured to use a certificate signed by the Certificate Authority (CA) that is in your browser’s list of trusted CAs.
Create a Transfer Site

The procedure below for adding a transfer uses the New Transfer Site page. This page provides full access to all transfer site configuration options. (If you want to exchange files with a single other user, you can also use Quick Add (page 19) to create a transfer site.)

Before you begin

- To add or edit a transfer site, you must be a member of the Transfer Site Administrators group (or any group with the Manage transfer sites role enabled).

To create a transfer site

1. Connect to the FileXpress Gateway Administrator (page 34).

   You see the Transfer Sites page. This page lists the sites you manage.

2. Click Add to open the New Transfer Site page.

3. Configure transfer directories.

   Transfer site name: This is the folder name users see when they connect to the Transfer Client.

   Directory name: This determines the name of the physical directory on the storage server, which is created in the base directory configured for this server. This directory is created when the first user logs into the site. By default, this value is filled in automatically with the transfer site name when you move your cursor. In most cases, you should use this default. Specify a different directory if you want your transfer to use an existing directory on the file storage server. Note: This existing directory must be relative to the base directory.

4. (Optional) Configure email notification. (To support email notification, email settings (page 67) must be configured by a FileXpress system administrator.)

   Send email notification: When this is enabled (the default), users you add to this transfer site are sent a transfer site access email notification when you save this site.

   Custom message: Use this optional field to add additional information to the email message. (The text you enter here replaces the $CUSTOM_MESSAGE$ token in the transfer site access email template.)

5. (Optional) Assign Post Transfer Actions (page 39).

   The Add Actions drop-down shows available Post Transfer Actions. The actions you select run only after a successful file upload to this site. If no actions are listed, it means that none have been configured.

6. Add one or more users to the site. Users you add will see this site when they connect to the FileXpress Transfer Client.

   Existing User: Use this area to add existing users or groups to the transfer site. They can be in the FileXpress directory, or in any additional LDAP directory that has been added by the FileXpress system administrator.

   New FileXpress User: Use this area to create new FileXpress users. New users are sent an account creation email in addition to a transfer site access email when you save this site. (This option might not be visible. You must have the Manage FileXpress users role enabled to view this area.)
7 (Optional) Configure email notification and user permissions.

**Notifications:** Use these icons to specify who will receive email notifications after file uploads (👍) and downloads (👎). Click an icon to enable or disable permissions. Pale gray icons indicate that a permission is disabled.

**Permissions:** Use these icons to specify who can upload files (👍), download files (👎), and manage the site (🔧). By default, all users are given both upload and download permissions and only the site creator is given management rights.

---

Note: Members of the Administrators group can view all transfer sites. Other users can view only those sites that they have permission to manage.

---

8 Click **Save**.

---

**Connect to the Transfer Client**

You can use any of the following methods to connect to the Transfer Client:

- Use links in email messages sent from FileXpress Gateway.
- From a web browser, enter the following URL, replacing `<FileXpress_proxy_host>` with the name or IP address of the FileXpress proxy host.

```
https://<FileXpress_proxy_host>:9492
```
- Administrators with access to the system on which the FileXpress Transfer Server is running can also connect to the FileXpress Proxy server, by launching the Transfer Client from the Windows Start Menu (or Apps list). It is installed under **Attachmate FileXpress Gateway > FileXpress Transfer Client**.

---

**Warning Messages**

When you connect to the Transfer Client, you make a secure HTTPS connection to the Transfer Server. This connection type requires the server to present a security certificate to your browser to authenticate the server. After the HTTPS connection is established, the Transfer Server uses Java to display the client in your browser window. You might see one or more of the following warning messages, depending on how the Transfer Server is configured and on your browser and Java security settings.

- **Browser certificate warning**

  This warning appears in the browser window before you see the login page. You see this warning if the Transfer Server is still using the default self-signed certificate that installs with FileXpress Gateway. The exact content of the certificate warning depends on which browser you are using.

  After the default FileXpress Gateway Administrator certificate is replaced with one signed by a well-known Certificate Authority (CA), this message is not displayed. It appears only when a certificate is presented that is not signed by a CA in the browser’s list of trusted CAs.

- **Browser permission to run Java**
Depending on your browser and whether you have used other Java applets, after you enter your user name and password you might see a request to allow Java to run. Look for an option such as "Enable," "Allow and Remember," or "Always run on this site" to allow Java to run without confirmation in the future.

- Java certificate warning

This dialog box appears after you have entered your user name and password. It includes the following note: "The certificate is not valid and cannot be used to verify the identity of this website."

After the default FileXpress Gateway Administrator certificate is replaced with one signed by a well-known Certificate Authority (CA), this message is not displayed. It appears only when a certificate is presented that is not signed by a CA that is included in Java's list of Secure Site CA certificates. (You can review and modify this list from the Java Control Panel.)

- Java confirmation messages

Java uses security messages to ensure that only software you approve runs on your system. These messages identify the publisher of the application and include a "Do not show this again" option. To connect to the Transfer Client without seeing these messages in the future, you can select this option after confirming that Attachmate is the publisher.

The Transfer Client User Interface

The sample Transfer Client connection shown below points out key features of the FileXpress Transfer Client user interface:
The image below shows a connection made by a user with access to two transfer sites:

- Use the up arrow to navigate up in the local file structure.
- Transfer site name
- Use drag and drop to transfer files
- The status line shows a successful connection

If you have access to multiple transfer sites, you see them as separate folders when you log in. Double-click a folder to transfer files to that site.
A Post Transfer Action (PTA) is a program that is invoked on the file storage server after a file has been successfully uploaded to the server. You can configure PTAs in Gateway Administrator or in a Reflection for Secure IT server that has been configured to act as the file storage server.

- **Post Transfer Actions configured in Gateway Administrator**
  PTAs configured in Gateway Administrator are associated with transfer sites. By default, new sites are added with no associated PTAs. The transfer site administrator can add any defined PTA to the transfer site. A PTA that has been added to a transfer site runs after each successful upload of a file to that site. This approach is appropriate when you want to configure different actions for different transfer sites, or when you want actions to follow uploads to some sites, but not others.

- **Post Transfer Actions in a Reflection for Secure IT server**
  This approach is available if you have configured Reflection for Secure IT for Windows as your file storage server. PTAs configured on this server are global. By default, Post Transfer actions act on all files uploaded to this server. A filter option is available that enables you to limit the action to all files that match the filter specification. For example, you might configure a post transfer action to act only on files with a *.exe extension. This approach is appropriate when you want to ensure that actions take place after all uploads. A typical use for this kind of PTA is running a virus scanner.

## Configure PTAs in Gateway Administrator

A Post Transfer Action (PTA) is a program that is invoked on the file storage server after a file has been successfully uploaded to the server. For example, you might configure a PTA in Gateway Administrator that renames or moves successfully uploaded files. Because these PTAs are assigned to individual transfer sites, you can configure site-specific actions.

**Characteristics of Post Transfer Actions configured on Gateway Administrator:**

- PTAs run on the file storage server. Review Supported File Storage Configurations below to ensure that your actions will have sufficient permissions to run on this server.

- PTAs are assigned to transfer sites. A PTA will run only after uploads to a site to which it has been added.
You can assign multiple Post Transfer Actions to a transfer site, but the order of actions in the transfer site definition does not control the order of execution for these actions. To ensure that a series of actions takes place in a predictable sequence, include the actions in a single script, then create a PTA that runs that script.

- Outputs from one PTA cannot be used as inputs to another PTA.
- Failed execution of a PTA does not prevent other PTAs from executing.
- PTAs are executed only after successful transfers. They do not run after unsuccessful or canceled transfers.
- PTAs are not supported for downloads or other file transfer events, such as renaming or deleting a file on the server.
- By default, up to 10 actions can execute simultaneously. Additional actions are added to a queue and executed as other actions are completed. You can modify this default in the Gateway Administrator properties file (page 88) using the configservice.event.threads setting.
- If the Gateway Administrator service or computer shuts down for any reason, unprocessed actions are processed when the service resumes.

**Supported File Storage Configurations**

Gateway Administrator PTAs run on the configured file storage server. Review the following to ensure that your Post Transfer Actions will have sufficient permissions to run.

The following configuration is recommended for running PTAs:

- Any configuration in which File Storage (page 62) has been configured to use an SFTP server.
  
  In this configuration, the PTA runs as a remote SSH command executed using the user account specified in the File Storage configuration.

---

Note: This is the only supported configuration for PTAs if you use a Gateway Administrator cluster (page 99).

The following configuration is supported with a modification to the FileXpress Gateway Administrator service:

- All FileXpress Gateway services are installed on the same computer and File Storage (page 62) is set to FileXpress proxy.
  
  In this configuration, the PTA runs as a local process and runs with the same privileges as the Gateway Administrator service. To run actions with this configuration, you need to modify the default privileges of the Gateway Administrator service (page 95).
The following configuration is likely to lead to permission and access problems and is not recommended:

- The FileXpress Proxy services and Gateway Administrator are installed on different systems and File Storage is set to FileXpress proxy.

To support this configuration, the FileXpress base path on the FileXpress Secure Shell Proxy must be configured with a UNC path. The UNC path can be to the same computer or a network share. PTAs are executed by Gateway Administrator, so the UNC path must be accessible by processes on the Gateway Administrator computer, and the Gateway Administrator service account must have privileges to run post transfer actions on the proxy.

To configure Post Transfer Actions in Gateway Administrator

1. Use the Actions tab to define a post transfer action (page 41).
2. Use the Transfer Sites tab to add the action to a transfer site (page 44).

Logging for Gateway Administrator PTAs

The log file for Gateway Administrator PTAs is the Gateway Administrator console log file. Output from the configured program or command is directed to this log. The log also includes Gateway Administrator error messages to help troubleshoot PTAs. The default location is:

C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\logs\console.yyyymmdd.log

Define a PTA in Gateway Administrator

You can configure a Post Transfer Action (PTA) to perform actions on files successfully uploaded to a transfer site.

- To add or edit PTAs, you must be a member of a group with the Manage actions role enabled.

- After a PTA is created, it will run only on transfer sites that have added it as an action. To add an action to a transfer site, you must have the Manage transfer sites role enabled; you do not need the Manage actions role to add an existing action.

Before you begin

- In Gateway Administrator’s File Storage (page 62) tab, configure an SFTP server and confirm that transfer sites can upload successfully to that server.
- OR-
- If you are using the default FileXpress proxy for file storage, change the privileges of the Gateway Administrator service (page 95).

To define a PTA

1. Connect to the FileXpress Gateway Administrator (page 34).
2. On the Actions tab, click New.
• For **Action name**, specify a descriptive name to identify this action.

• For **Program**, specify an executable command or the full path and name of an executable file on the file storage server. Some examples are provided below.

• (Optional) For **Arguments**, enter one or more arguments to be passed to the specified program. Arguments can include supported tokens (page 46). Tokens are replaced by actual values when the PTA runs.

3  Click **Save**.

**Examples**

Use these examples as models for testing and configuring PTAs. Samples include appropriate syntax for both Windows and UNIX SFTP servers.

**Example 1: Send a directory listing to the log file**

This example uses a system command to send a directory listing to the Gateway Administrator log file (page 112). The `$FILE_PATH$` token is used to get the listing for the upload directory. Because the destination directory might include spaces, this token is enclosed in double quotation marks.

**Windows SFTP server**

Program: cmd

Arguments: /c dir "$FILE_PATH$"

Note: Use the /c argument when you use the Windows cmd command. This switch specifies that cmd should exit after the specified command is carried out.

**UNIX SFTP server**

Program: ls

Arguments: -a -l "$FILE_PATH$"

**Example 2: Copy uploaded files to a specified directory**

This example uses a system command to copy uploaded files to an existing destination directory.

Note: The destination directory (fxgout in these examples) must exist, and the user account specified in the **File Storage** (page 62) configuration must be able to write to this directory.

**Windows SFTP server**

Program: cmd

Arguments: /c copy "$FULL_PATH$" c:\fxgout
UNIX SFTP server

Program: cp

Arguments: "FULL_PATH" /fxgout

Example 3: Use a script to perform a sequence of actions

This example uses a script to write information about the transfer to a file, and then move the file to a specified directory. File tokens are passed to the script as command line arguments. Because the returned values of these tokens can include spaces and special characters, the arguments are enclosed in double quotes.

Note: The user account specified in the File Storage (page 62) configuration must have sufficient rights to run the script and write to the output directories (fxgpta and fxgout in these examples).

Windows SFTP server

The PTA runs the script demo.bat, which adds information about each transferred file to the filelist.txt file, then moves the uploaded files to c:\fxgout.

Program: c:\fxgpta\demo.bat

Arguments: "FILENAME" "TIME" "INITIATOR_USERID" "FULL_PATH"

Contents of demo.bat:

```
echo Filename: %1 >> c:\fxgpta\filelist.txt
echo Transfer Time: %2 >> c:\fxgpta\filelist.txt
echo User ID: %3 >> c:\fxgpta\filelist.txt
echo ================= >> c:\fxgpta\filelist.txt
move %4 c:\fxgout
```

UNIX SFTP server

The PTA runs the script demo.sh, which adds information about each transferred file to the filelist file, then moves the uploaded files to /fxgout.

Program: /fxgpta/demo.sh

Arguments: "FILENAME" "TIME" "INITIATOR_USERID" "FULL_PATH"

Note: A common error is to forget to set execute permissions on the script file using chmod. For this example execute permissions were set using: chmod +x demo.sh.

Contents of demo.sh:

```
echo Filename: $1 >> /fxgpta/filelist.txt
echo Transfer Time: $2 >> /fxgpta/filelist.txt
echo User ID: $3 >> /fxgpta/filelist.txt
echo ================= >> /fxgpta/filelist.txt
move $4 /fxgout
```
Add a PTA to a Transfer Site

To run a post transfer action (PTA), you need to add the action to a transfer site. After a PTA has been added to a transfer site, if the PTA is enabled (the default), it will act on all files that are successfully uploaded to that site. Post transfer actions do not run after uploads to transfer sites that have no added actions.

- To add or edit the actions associated with a transfer site, you must be a member of a group with the Manage transfer sites role enabled.

Before you begin

- One or more PTAs must already be defined (page 41).

To add a PTA to a transfer site

1. Connect to the FileXpress Gateway Administrator (page 34).
2. On the Transfer Sites tab, click New or select an existing site and click Edit.
3. Use the Add actions drop-down list to select the action or actions you want to add. Added actions appear below the drop-down list. Click the X in any added action to remove that action.

Note: You can assign more than one post transfer action to a transfer site, but the order of actions in the transfer site page does not control the order of execution for these actions. To ensure that a series of actions takes place in a predictable sequence, include the actions in a single script or batch file.

4. Click Save.

Configure PTAs in Reflection for Secure IT

If you have configured Reflection for Secure IT (version 8.2 or later) as your file storage server, you can set up Post Transfer Actions directly on this server. PTAs created this way are global; they act on all uploaded files by default and are not associated with transfer sites. A typical use for this kind of PTA is running a virus scanner.

PTAs configured on the Reflection for Secure IT server run under the same account as the Reflection for Secure IT service (the Local System account). This account has administrative privileges on the local system.

- By default, Post Transfer actions act on all files uploaded to this server. A filter option is available that enables you to limit the action to all files that match the filter specification.

- You can configure multiple PTAs, but the order of actions in the Post Transfer Actions pane does not control the order of execution for these actions. To ensure that a series of actions takes place in a predictable sequence, include the actions in one batch file.

- Outputs from one PTA cannot be used as inputs to another PTA.

- Failed execution of a PTA does not prevent other PTAs from executing.
PTAs are executed only after successful transfers. They do not run after unsuccessful (or canceled) transfers.

PTAs are not supported for downloads or other file transfer events (such as renaming or deleting a file on the server).

By default, up to 50 actions can execute simultaneously. You can modify this default on the Post Transfer Actions pane.

Logging for Reflection for Secure IT PTAs

Error messages and PTA output can be viewed in either the Windows Event Viewer or the server's debug (text) log file. Windows Event logging is enabled by default, but the default logging level does not include the PTA output; you need to increase the logging level to "Information" to see this content. Debug logging is not enabled by default. For working with PTAs, enabling debug logging to a text file is recommended.

To configure PTA logging to a text file on a Reflection for Secure IT Server

1. From the Reflection for Secure IT Configuration tab, click Debug Logging.
2. Click Enable debug logging to log file. By default, this log is set to Information, which is sufficient to include PTA output and error messages.

   You can click Custom to fine-tune the level of output that is sent to this log. Three settings control PTA output: LOG_I_PTA_ERROR, LOG_I_PTA_RESULT, and LOG_T_PTA.
3. Save your settings (File > Save Settings).

To view the text log file

- From the Reflection for Secure IT console View menu, select View Latest Debug Log File.

Define a PTA in Reflection for Secure IT

If you have configured Reflection for Secure IT as your file storage server, you can add Post Transfer Actions to this server.

Before you begin

- Install the Reflection for Secure IT server (page 11).
- In the Reflection for Secure IT console, enable debug logging to a text file.
- In the Gateway Administrator File Storage (page 62) tab, select SFTP server and configure a connection to your Reflection for Secure IT server. Confirm that transfer sites can upload successfully to this server.

To configure Post Transfer Actions in Reflection for Secure IT

1. From Reflection for Secure IT console, go to Configuration > Post Transfer Actions.
2. Click Add to create a new PTA.
For information about configuring **File filter**, **Program**, and **Arguments**, refer to the dialog box help and the examples below.

3  Save your settings (**File > Save Settings**).

### Examples

Use these examples as models for testing and configuring PTAs.

#### Example 1: Send a directory listing to the log file

This example sends a directory listing to the log file. The default file filter triggers the action after every upload. The program for these PTAs must be specified using the full path; in this example it is the path to the Windows `cmd` command. The `$FILE_PATH$` token is used to get the listing of the upload directory. Because the destination directory might include spaces, this token is enclosed in double quotation marks.

- **File filter:** `.*`
- **Program:** `C:\Windows\System32\cmd.exe`
- **Arguments:** `/c dir "$FILE_PATH$"

---

**Note:** Use the `/c` argument when you use the Windows `cmd` command. This switch specifies that `cmd` should exit after the specified command is carried out.

#### Example 2: Copy uploaded PDF documents to specified directory

This example copies uploaded PDF files to an existing destination directory. The file filter uses a regular expression to specify all files with a `.pdf` file extension.

- **File filter:** `.*\.pdf`
- **Program:** `C:\Windows\System32\cmd.exe`
- **Arguments:** `/c copy "$FULL_PATH$" c:\fxgout

### Post Transfer Action Tokens

Post Transfer Actions tokens can be passed as command line arguments to the PTA executable. These tokens are replaced by actual values based on the file transfer.

- Tokens must be preceded and followed by a dollar sign ($), for example `$TIME$`.
- You can enclose tokens in quotation marks. This might be required to pass arguments that include spaces or special characters.
The following tokens are available:

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
<th>Sample Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLIENT_IP</td>
<td>The IP address of the client system.</td>
<td>fe80::21a5:4df7:fdce:6951</td>
</tr>
<tr>
<td>DATE</td>
<td>The date of the transfer. The format for the date is determined by the locale setting of the server.</td>
<td>05/28/2014</td>
</tr>
<tr>
<td>FILENAME</td>
<td>The name of the uploaded file.</td>
<td>myfile.txt</td>
</tr>
<tr>
<td>FILE_HASH</td>
<td>The SHA-1 hash of the uploaded file.</td>
<td>ebd90566a6a5d7c66a784839cab05b08949a9141</td>
</tr>
<tr>
<td>FILE_PATH</td>
<td>The path—without the filename—to the destination directory on the file storage server.</td>
<td>C:\Base directory\FileXpress\transfersite</td>
</tr>
<tr>
<td>FILE_SIZE</td>
<td>The file size (in bytes).</td>
<td>7326</td>
</tr>
<tr>
<td>FULL_PATH</td>
<td>The full path—including the filename—of the destination file on the file storage server.</td>
<td>C:\Base directory\FileXpress\transfersite\myfile.txt</td>
</tr>
<tr>
<td>INITIATOR_EMAIL</td>
<td>The email of the client user that uploaded the file.</td>
<td><a href="mailto:joe@acme.com">joe@acme.com</a></td>
</tr>
<tr>
<td>INITIATOR_USERID</td>
<td>The domain and user ID of the client user that uploaded the file, in the format: domain\user.</td>
<td>mydomain\joe</td>
</tr>
<tr>
<td>TIME</td>
<td>The time of the transfer on the FileXpress Secure Shell Proxy.</td>
<td>14:26:59</td>
</tr>
<tr>
<td>TIMEZONE</td>
<td>The time zone of the FileXpress Gateway Administrator.</td>
<td>-0700</td>
</tr>
<tr>
<td>TRANSFER_SITE_NAME</td>
<td>The Transfer site name from New/Edit Transfer Site (page 49).</td>
<td>Accounting department files</td>
</tr>
</tbody>
</table>

* - Supported in Gateway Administrator PTAs, but not in Reflection for Secure IT PTAs.
Transfer Sites

Use this page to view and manage FileXpress Gateway transfer sites. Note the following:

- To view the Transfer Sites page, you must be a member of a group with the Manage transfer sites role enabled.
- Members of the Administrators group can view all transfer sites. Other users can view only those sites that they have permission to manage.
- Click on a column heading to sort the list based on the entries in that column.
- To select multiple transfer sites, click multiple check boxes, or use Shift+click to select a range of currently visible sites.

Quick Add      Opens the Quick Add dialog box. This provides a quick way to create a new transfer site and add a user to the site. If the user email you specify doesn't yet exist in the FileXpress user list, you see a confirmation message asking if you want to add the user. When you OK this message, a registration email is sent to the user.

Add     Opens New Transfer Site (page 49). This page provides complete site creation options for creating a new transfer site.

Edit       Available when one site is selected.

Delete     Deletes the selected site or sites.

---

Note: To use this option, you must be a member of the Transfer Site Administrators group (or any group that has both Manage FileXpress users and Manage transfer sites enabled).
# Transfer Site Configuration

Use the Transfer Site page to create or edit a transfer site, modify the list of users who can use this site, and configure permissions for members of this site.

- To view this page and create or edit transfer sites, you must be a member of a group with the **Manage transfer sites** role enabled.

## Site Configuration Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transfer site name</strong></td>
<td>This name is visible to users of the site when they connect using the FileXpress Transfer Client. The site name must be unique. If you specify the name of an existing site, you'll see an error message when you try to save the site.</td>
</tr>
<tr>
<td><strong>Directory name</strong></td>
<td>The name of the physical directory to be used by this site on the file storage server (page 62). It is created in the base directory configured for this server. By default, this value is filled in automatically with the transfer site name when you move your cursor. In most cases, you should use this default. Specify a different folder if you want your transfer to use an existing directory on the file storage server. Note: This existing directory must be relative to the base directory. The directory name must be unique. If you specify the name of an existing directory, you'll see an error message when you try to save the site.</td>
</tr>
<tr>
<td><strong>Delete directory when transfer site is deleted</strong></td>
<td>Note: This setting applies only when the file storage server is set to <strong>SFTP server</strong>. Sites on the FileXpress Proxy are not deleted, regardless of the value of this setting. When this option is selected, the physical directory on the SFTP server, and any files it contains, are deleted when the transfer site is deleted. When this option is not selected (the default), the physical directory and its contents remain on the file storage. If a new site is created using the same directory name as a deleted site, users added to the site will be able to view and transfer any files remaining from the deleted site.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>An optional description of this site. This description can be added to the Transfer site access email using the <code>$TRANSFER_SITE_DESCRIPTION$</code> token.</td>
</tr>
<tr>
<td><strong>Expires</strong></td>
<td>When set to <strong>Yes</strong> (the default), the site expires at the specified date. Expired sites remain in the database, but are not available to Transfer Client users. To restore an expired site, reset the expiration date to a future date. The default expiration is 2 years (730 days) after the site is created. This default is configurable in the Gateway Administrator properties file (page 88).</td>
</tr>
<tr>
<td><strong>Send email notification</strong></td>
<td>When set to <strong>Yes</strong> (the default), a Transfer site access email is sent to each user added to the site when you save the site. This option must be enabled at the time users are added to the site. Changing this setting from No to Yes will not result in emails to any users who have already been added and saved as members of the site.</td>
</tr>
</tbody>
</table>
**Custom message**  This option is available when **Send email notification** is enabled. The message entered here replaces the $CUSTOM_MESSAGE$ token in the Transfer site access email.

**Add actions**  If Post Transfer Actions (page 57) are available, they appear in this drop-down list. Post Transfer Actions are executed after a successful file upload. They are not available for downloads or unsuccessful transfers.

---

**Existing User**

Under **Existing User**, add existing users or groups to the transfer site. They can be in the FileXpress directory or in any additional LDAP directory that has been added by the FileXpress system administrator.

**LDAP Server**  Select the directory that you want to search.

**Users/Groups**  Select whether you want to search for users or groups.

**Search users...**  Typing in this field initiates a search for users or groups in the selected LDAP server. Note the following:

- The results list shows first and last names (if present) and email. Although the userID is also included in the search, it isn't displayed in the results list.
- The results list is limited to 10 users. If the user is not visible, continue to enter more of the user's name.
- The user or group you select is not added to the list until you click **Add**.

**Add**  This button is available after you have specified a valid user or group. Click it to add the user or group to the transfer site list. Users or groups you add to this list are added to the transfer site when you click **Save**.

---

**New FileXpress User**

Under **New FileXpress User**, add users who are not yet provisioned. New users are sent an Account creation email when you save this site. You must have the Manage FileXpress users role enabled to view this area.

**Note:** This feature relies on email registration for new users. Configure email support (page 17) and test email notification before using this option. If email support is not correctly configured, the account is created, but the user will not receive an account creation email. If users are not receiving email messages, see Email Troubleshooting (page 119).

**User email**  When you add a user here, the email address also becomes the user's UserID. Required.
First name       Optional.

Last name       Optional.

Add

Add the new user to the list of transfer site members.

Users you add to the list this way are added to the transfer site and the FileXpress directory when you click Save.

User / Group

This list shows the currently configured members of the transfer site.

- To remove any member of the list, click the X to the left of the user or group name.

User / Group       The name of users and/or groups that have been added to this site.

LDAP Server       The LDAP server that the user or group is a member of.

Notifications

Use these icons to view and edit when each or group receives email notifications.

Click an icon to enable or disable notification. Pale gray icons indicate that notification is disabled.

An email is sent each time a file is uploaded to this site.

An email is sent each time a file is downloaded from this site.

Permissions

Use these icons to view and edit what permissions each user or group has. Pale gray icons indicate that a permission is disabled. For example, a user with the following permissions can download files, but cannot upload files or manage the site.

Click an icon to enable or disable permissions.

The user can upload files to the site.

The user can download files from the site.

The user is a site manager and can modify site settings and membership. By default, only the user who creates the site has this permission enabled. Site managers must be a member of the Transfer Site Administrators group (or any group that has Manage transfer sites enabled).

Members of the Administrators group can view and manage all transfer sites. Other users can view only those sites that they have permission to manage.
Users

Use this page to view and manage FileXpress users. These users can log into the FileXpress Transfer Client and access any transfer sites that they are members of.

- To view the Users page, you must be a member of a group with the Manage FileXpress users role enabled.
- If Gateway Administrator has an external LDAP directory configured, select the directory name in the drop-down list next to LDAP Server to view these users. The user list is read-only for users in added LDAP directories; all passwords and identifying information for these users is managed on the LDAP server.
- The LDAP server might set a limit on the number of users that can be listed. This limit affects only the number of users who can be listed and viewed, not the number of users who are provisioned. If the list does not display all users, use the Filter User option to view users who are not visible in the default list.
- The Expires column is visible only when LDAP server is set to FileXpress.
- Click on a column heading to sort the list based on the entries in that column.
- To select multiple users, click multiple check boxes, or use Shift+click to select a range of currently visible users.

LDAP Server  Specifies which LDAP directory to display. The built-in FileXpress directory is available and selected by default. The FileXpress administrator can add additional directories from LDAP Servers (page 58).

New  Open New User (page 52).

Available only when LDAP server is set to FileXpress.

Edit  Open Edit User (page 53) to edit the selected user.

Available only when LDAP server is set to FileXpress and only a single user is selected.

Delete  Delete the selected user or users.

Available only when LDAP server is set to FileXpress.

You cannot delete the administrator account that you are currently logged in as.

Filter User  Search the selected directory for users that contain the entered string.

Clear  Removes the filter and lists all users in the selected directory.

New User

Use this page to add a new user to the built-in FileXpress LDAP server.
To view the New Users page, you must be a member of a group with the Manage FileXpress users role enabled.

Red asterisks mark required fields.

**UserID**
The user's login name. Required. This can be the same as the user email address.

User ID is not case-sensitive. It must be between 1 and 64 characters in length, and cannot contain the characters `<`, `>`, `:`, `|` or these character sequences: CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, and LPT9.

**Email address**
Required.

**First name**
Optional.

**Last name**
Optional.

**Email registration**
When you click Save, the new user is sent an Account creation email that includes a time-limited link for setting a password.

Note: Configure email support (page 17) and test email notification before using this option. If email support is not correctly configured, the account is created, but the user will not receive an account creation email. If users are not receiving email messages, see Email Troubleshooting (page 119).

**Specify password**
If you select this option, no email is sent from FileXpress Gateway to your users; you need to manually communicate user name and password information.

**Require password change**
After this user logs in with the initial password, the user will be prompted immediately to change the password.

**Expires**
When set to Yes (the default), the user account expires at the specified date.

You can disable an account by setting a date in the past. To enable an expired account, set a date in the future.

By default, new FileXpress user accounts are set to expire two years after they are created. This default can be changed by editing the Gateway Administrator properties file (page 88).

**FileXpress group membership**
Use the selection box to add this user to any available group. Added groups, and the roles the user inherits from these groups, are displayed under the selection box.

Group membership is optional.

---

**Edit User**

See New User (page 52) for information about items on this page. Note the following differences:
You cannot edit the **UserID** on the **Edit User** page.

Click **Change Password** to display the password change options.

Email notification is not available for edits to user accounts.

**Groups**

Use this page to view and manage FileXpress Gateway groups. You can use groups to add members to transfer sites and to configure roles for Gateway Administrator users.

- The default Administrators group has all roles enabled. In addition, users in this group can see and manage all transfer sites. You cannot delete this group, nor can you delete the last member of this group.

- The default Transfer Site Administrators group has **Manage user** and **Manager transfer sites** roles enabled.

- To view the **Groups** page, you must be a member of a group with the **System setup** role enabled.

- To view the groups in an added LDAP directory, select the directory name in the drop-down list next to **LDAP Server**. The group list is read-only for groups in added LDAP directories; these groups are managed on the LDAP server.

- Click on a column heading to sort the list based on the entries in that column.

- To select multiple groups, click multiple check boxes, or use Shift+click to select a range of currently visible groups.

**LDAP Server**

Specifies which LDAP directory to display. The built-in FileXpress directory is available and selected by default. The FileXpress administrator can add LDAP directories using **LDAP Servers** (page 58).

**New**

Opens **New Group** (page 54).

Available only when **LDAP server** is set to FileXpress.

**Edit**

Opens **Edit Group** (page 55).

Available only when **LDAP server** is set to FileXpress and only when a single group is selected.

**Delete**

Available only when **LDAP server** is set to FileXpress.

You cannot delete the Administrators group.

**Filter Group**

Search the selected directory for groups that contain the entered string.

**Clear**

Clears the filter.

**New Group**

Use this page to add a new group to the FileXpress directory.
To view the **New Group** page, you must be a member of a group with the **System setup** role enabled.

You cannot modify the member list from the **New Group** page. You can modify the members list from the **Edit Group page**. Or, add individual users to a group from the **Edit User** page.

- **GroupID**
  Required. Cannot contain any of the following characters: <>:\?*

- **Description**
  Required.

- **Roles**
  Specify which roles (page 27) are available to users in this group.

### Edit Group

Use this page to modify FileXpress groups. Groups in added LDAP servers are read-only; they must be managed on the LDAP server.

- To view the **New Group** page, you must be a member of a group with the **System setup** role enabled.

  - **GroupID**
    GroupID is read-only when you are editing an existing group.

  - **Description**
    Length must between 1 and 256 characters.

  - **Roles**
    Specify which roles (page 27) are available to users in this group.

---

**Note:** Changes to the above settings are saved to the database when you click **Done**. Changes to the group membership are saved to the database automatically when you complete the action.

---

### Members

- **Add Members**
  Opens **Add Members** (page 56), which you can use to add one or more users to the group.

- **Remove**
  Removes the selected user or users from the group.

- **Filter Members**
  Enter text in the text box and click **Filter Members** to search for users.

- **Clear**
  Clears the filter.

In some situations, users that have been added to a group might no longer be available. This can happen if a user has been removed from the remote LDAP server directory, or if you edit the **Base DN** or **LDAP filter** settings for the LDAP server. When a group member is no longer available, the **UserID** in the list is replaced by the Distinguished Name that identified that user, and the user is identified as "(Not Available)". For example:

CN=Joe Green,OU=Users,OU=sales,DC=acme (Not Available)

Users marked as not available can become available to the group if the LDAP server conditions change again. Or, you can delete these users from the group if you don't want them to remain in the list.
Add Members

Getting there

1. Log into Gateway Administrator as a member of a group that has the System setup role enabled.
2. Click Groups.
4. Select the check box next to a group and click Edit.
5. Click Add Members.

Use this page to add members to any group in the built-in FileXpress LDAP server.

- You can add users from any LDAP Server to your FileXpress groups.
- To select multiple users, click multiple check boxes, or use Shift+click to select a range of currently visible users.
- Changes to the group membership are saved to the database automatically when you complete the action.

LDAP Server  Specifies which user directory to display. The list of users shows users who are not yet members of the group you are editing.

Filter User  Search for users in the listed directory using the text you enter in the search box.

Clear  Clears the filter and displays all users of the selected directory who are not already members of the group.

Actions

Use this page to view and edit Post Transfer Actions (page 39).

- To view the Actions page, you must be a member of a group with the Manage actions role enabled.

Post Transfer Actions (PTAs) run on the file storage server. Setting File Storage (page 62) to an SFTP server is the recommended configuration for running PTAs. In this configuration, each PTA runs as a remote SSH command, executed using the privileges of the user account specified in the File Storage configuration.

To support PTAs when File Storage is set to FileXpress proxy (the default), install all FileXpress Gateway services on the same computer and modify the default privileges of the Gateway Administrator service (page 95).
**Action Configuration**

Use this page to configure Post Transfer Actions (PTAs).

- To view the **Action** page, you must be a member of a group with the **Manage actions** role enabled.

**Action name**  Specify a descriptive name to identify this action. The name you specify here is shown in the list of available actions when you configure a transfer site.

**Program**  Specify a system command supported on the file storage server, or the full path and name of an executable file on that server. For examples, see Define a PTA in Gateway Administrator (page 41).

**Arguments**  (Optional) Enter one or more arguments to be passed to the specified program. Arguments can include supported tokens (page 46) (enclosed in dollar signs). Tokens are replaced by actual values when the PTA runs.

- Use spaces to separate multiple arguments.
- Use double quotation marks around any argument that might include spaces in the returned value.

**Tokens**  Click this button to insert a token from a list of supported tokens (page 46).

**System**

To view and edit **System** settings, you must be a member of a group with the **System setup** role enabled.

**In this Section**

- LDAP Servers Tab  58
- LDAP Server Configuration  58
- Email Server Tab  60
- Email Templates Tab  61
- File Storage Tab  62
- Authentication Tab  63
- PKI Servers Tab  64
- PKI Server Configuration  64
LDAP Servers Tab

Getting there

1. Log into Gateway Administrator as a member of a group that has the System setup role enabled.

2. Go to System > LDAP Servers.

You can add users to FileXpress Gateway by adding one or more LDAP servers to Gateway Administrator. Authentication and group membership are managed on the LDAP server. Each time the user logs in, current information is retrieved from the LDAP server.

- Windows Active Directory is the only LDAP directory type supported in version 1.0.
- FileXpress is the built-in LDAP server. You cannot delete this server and you cannot modify it from this page. Click the Users tab to add or delete users in the FileXpress directory.

LDAP Server Configuration

Use this page to configure connections to an LDAP server.

- You must click Save to save these settings. The Test Connection button verifies the connection, but does not save your settings.
- Red asterisks mark required fields.

<table>
<thead>
<tr>
<th>Type</th>
<th>Active Directory. This is not configurable; Windows Active Directory is the only LDAP directory type that is currently supported.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name</td>
<td>The domain name for this LDAP server.</td>
</tr>
<tr>
<td>Server</td>
<td>LDAP Server address. This can be a specific server name (myserver.mydomain.com), an IP address (10.10.123.123), or the domain address (mydomain.com).</td>
</tr>
<tr>
<td>Port</td>
<td>Port used by the LDAP server. 3268 is the default, and is standard for Active Directory global catalog for non-secure connections (LDAP). 3269 is the default for secure Active Directory global catalog for secure connections (LDAPS). Use of the default global catalog ports is recommended for better performance. For connections without using global catalog, 389 is standard for non-secure connections and 636 is standard for secure connections.</td>
</tr>
</tbody>
</table>
Clicking **Advanced domain settings** expands the display to show the following options. Use these settings to customize how FileXpress Gateway manages user authentication to this LDAP server. For additional information, see LDAP Server Advanced Domain Settings (page 29).

Note: **Advanced domain settings** apply to password authentication only; X.509 certificate authentication always requires user mapping that specifies both a domain and username.

### Domain mappings
If you have multiple LDAP servers configured, you can use this option to map the value in **Domain name** to these servers. This can improve performance, because FileXpress authenticates first against the servers you specify here.

### Remove user domain
When set to Yes, any domain name the user enters at login is removed before FileXpress Gateway authenticates the user to this LDAP server. For example, if a user enters `acme\joe`, the domain name `acme` is removed. If no **Default user domain** is specified, only the user ID `joe` is sent to the server for authentication.

### Default user domain
Specifies a default domain name to include when FileXpress authenticates users to this LDAP server. For example, if you specify `domain1` and a user logs in as `user_name`, the user is authenticated as `domain1\user_name`. This can be used in combination with **Remove user domain** to replace any domain name that the user includes with the value you specify here.

### UserID
Name of a user who has read access to this LDAP directory. You must include the user's domain. For example:

- `mydomain\user`
- `user@mydomain`
- `user@mydomain.com`

### Password
The LDAP user's password

### Base DN
The base DN under which users are located.

For example:

```
OU=Users,DC=mydomain,DC=com
```

### LDAP Filter
(Optional) Limits the list of users added to Gateway Administrator to those included in the specified filter. If no filter is specified, all users in the specified Base DN are added.

Use standard LDAP filter syntax. This example retrieves users in the group `myGroup`:

```
(\&\&\&\{objectCategory=user\}(memberOf=CN=myGroup,OU=Users,DC=mydomain,DC=com)\&\&\&\{objectCategory=group\}(CN=myGroup))
```
**Secure Connection**

Select this option to connect to the server using LDAP over SSL (LDAPS).

To make a successful secure connection, you must enable **Secure Connection**, provide the correct **Port** for LDAPS connections to this server (the port changes to 3269 by default), and use **Add Certificate** to browse to the certificate for this server. After you retrieve a certificate, information about that certificate will be displayed on the page.

---

**Email Server Tab**

**Getting there**

1. Log into Gateway Administrator as a member of a group that has the **System setup** role enabled.

2. Go to **System > Email Server**.

Email server configuration is required to support outgoing email messages sent from FileXpress Gateway.

**Test Connection**

Tests whether the specified SMTP server can be reached at the specified port.

This test does not confirm that outgoing messages will be successful. After your email server configuration is complete, you can use the Preview feature on the Email Templates (page 61) page to test an outgoing email.

This tests the current on-screen settings. These settings are not saved until you click **Save**.

**Save**

Saves the current settings. This button is not enabled until you have entered all required information.

Certificate information is saved automatically, but other edits are not saved until you click **Save**.

Moving to a new page without clicking Save cancels your edits.

**Email Service**

Select **Enabled** to enable email emails from Gateway Administrator.

**SMTP server**

The name or IP address of the outgoing email server.

This field and the other items on this page cannot be edited if **Email service** is **Disabled**.

**Port**

The listening port on the SMTP server.

This setting changes automatically when you change the **Secure connection** setting to match the standard port for each option. If your server uses a non-default port, change the port value after selecting your secure connection type.

**UserID**

Some SMTP servers require user credentials to support sending outgoing messages. Use these fields to enter valid user credentials.
### Email Templates Tab

**Getting there**

1. Log into Gateway Administrator as a member of a group that has the **System setup** role enabled.

2. Go to **System > Email Templates**.

Use this tab to customize the email notifications sent from FileXpress Gateway.

<table>
<thead>
<tr>
<th><strong>Template list</strong></th>
<th>Use this drop-down list to select the template you want to edit. See Email Notifications (page 67) for a description of when each template is used.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User type</strong></td>
<td>Select <strong>FileXpress user</strong> to customize templates that are sent to users added to the FileXpress LDAP server. Select <strong>LDAP server</strong> to edit templates sent to users in an added LDAP server.</td>
</tr>
<tr>
<td></td>
<td>The default templates are the same for both groups, with the exception of the Password Request template.</td>
</tr>
<tr>
<td></td>
<td>Account Creation and Password Reset are not available for LDAP users.</td>
</tr>
<tr>
<td><strong>Import</strong></td>
<td>Opens a browse dialog box that you can use to import content from a file created with a text or HTML editor.</td>
</tr>
<tr>
<td><strong>Restore Default</strong></td>
<td>Restores the default content for the selected template.</td>
</tr>
<tr>
<td><strong>Sender address</strong></td>
<td>Emails that use the selected template will show that they are from this email address. You can use the default token or delete the token and enter an email address here. Some email servers require that this be a valid user.</td>
</tr>
<tr>
<td></td>
<td>The GLOBAL_SENDER_ADDRESS token enters the <strong>Sender address</strong> value specified in the <strong>Email Server</strong> tab.</td>
</tr>
<tr>
<td><strong>Sender name</strong></td>
<td>Emails that use the selected template will show that they are from this user.</td>
</tr>
<tr>
<td></td>
<td>The GLOBAL_SENDER_NAME token enters the <strong>Sender name</strong> value specified in the <strong>Email Server</strong> tab.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>The subject line that will appear in the email.</td>
</tr>
</tbody>
</table>
**Insert token**

Use this list to insert a token (page 70) in the current cursor position in the message body. Tokens must be preceded and followed by a dollar sign ($). The dollar signs are added automatically when you use **Insert token**. You can also type token values manually.

The list shows the tokens that are supported for the currently selected template.

Tokens for which no value is available are omitted from email messages.

**Body of message**

The body can be provided in text or HTML format.

You can edit this area directly, or use **Import** to import content from a file created with a text or HTML editor.

**Preview**

Click the Preview heading or the arrow to expand the preview area.

Tokens in the preview are replaced by sample content enclosed in square brackets. For example: [myTransferSite]. In actual generated email, the brackets do not appear and the sample content is replaced by actual content.

To send a test email, enter an email address in the **To** field and click **Send Test Email**. This test can help you determine if your email server is correctly configured and supports your current values for Sender address and Sender name.

**File Storage Tab**

Getting there

1. From Gateway Administrator, go to **System > File Storage**.

Use this page to designate a file storage server to be used for FileXpress Gateway transfer sites. Files for each transfer site you create are placed in a subdirectory of the designated base directory on the file storage server.

**Note:** The name and location of the base directory you configure for your file storage server is not made visible to client users. The folder name that users see when they connect is the value you specify for **Transfer site name** when you create a transfer site. The actual subdirectory on the file storage server is the value you specify for **Directory name**.

**FileXpress proxy**

When this option is selected, transfer site directories are created on the FileXpress Gateway Proxy. The default base directory on this server is:

C:\ProgramData\Attachmate\RSecureServer\FileXpress\

This base directory can be modified from the FileXpress Gateway Proxy computer using the FileXpress Secure Shell Proxy console. For details, see **Configure File Storage on the FileXpress Proxy** (page 73).

**SFTP server**

Selecting this option displays settings for configuring a connection to an SFTP server. Transfer site directories are created on the specified SFTP server.
The SFTP server configuration options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The name or IP address of the SFTP server. This can be a Reflection for Secure IT Server for Windows (available for install using the FileXpress Gateway setup program) or another SFTP server running any platform.</td>
</tr>
<tr>
<td>Port</td>
<td>The port used for SFTP and SSH connections on the server. Port 22 is the standard.</td>
</tr>
<tr>
<td>Host key fingerprint</td>
<td>Connections to the SFTP server require host authentication using a public key. Once you have specified a server and port, you can click Retrieve to import this key. The host key fingerprint displays the SHA1 hash of the retrieved key.</td>
</tr>
<tr>
<td>UserID</td>
<td>Specify a valid user account on the SFTP server. FileXpress Gateway uses the credentials of this account to access the file system on this server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the specified user.</td>
</tr>
<tr>
<td>Base directory</td>
<td>Specify the base directory under which FileXpress transfer site directories will be created. Click Browse to connect to the server and select a location. This automatically enters a path using the correct syntax for your server type. By default, the base directory is set to a subdirectory called FileXpressGateway in the directory you selected. This is not required; you can edit or delete this subdirectory name. Note: The directory you select must be available to the specified user account.</td>
</tr>
</tbody>
</table>

**Authentication Tab**

Getting there

1. Log into Gateway Administrator as a member of a group that has the **System setup** role enabled.
2. Go to **System > Authentication**.

Use this tab to determine how users authenticate when they log into the FileXpress Transfer Client.

- Changes made here apply to all users; it is not possible to configure password authentication for some users and certificate authentication for others.
- Before you can use X.509 certificate authentication, you must have at least one configured PKI Services Manager running, and you need to add it to the Gateway Administrator’s **PKI Servers** list. Reflection PKI Services Manager provides certificate verification services, and is available as a separate download from the FileXpress Gateway download page at no additional charge. For information about downloading PKI Services Manager and configuring it for use with FileXpress Gateway, see Set Up PKI Services Manager (page 32).
- Changes made here require a restart of the FileXpress Transfer Server. By default, this restart will occur within one minute after you save your change. (This update interval is configurable in the FileXpress Transfer Server properties file (page 90) using the servletengine.ssl.updateInterval setting.)
PKI Servers Tab

Getting there

1. Log into Gateway Administrator as a member of a group that has the System setup role enabled.

2. From Gateway Administrator, go to System > PKI Servers.

Reflection PKI Services Manager provides certificate verification services, and is available as a separate download from the FileXpress Gateway download page at no additional charge. For information about downloading PKI Services Manager and configuring it for use with FileXpress Gateway, see Set Up PKI Services Manager (page 32). To support X.509 certificate authentication, at least one PKI Server must be configured.

Note: You can install and configure PKI Services Manager on multiple systems to ensure availability of certificate authentication services. When you add multiple servers to the PKI Servers list, Gateway Administrator contacts the first available server on the list. The reply from this PKI Server (valid or not valid) is used, and no other servers on the list are contacted. All PKI servers must have identical trust anchors, configuration settings, and mapping files to ensure that each of your PKI Services Manager servers returns the same validation for all certificates.

New

You must have PKI Services Manager installed and running before you add it to the PKI Servers list.

Edit

This button is available when a PKI server is selected. Use it to disable the selected server or modify settings.

PKI Server Configuration

Getting there

1. Log into Gateway Administrator as a member of a group that has the System setup role enabled.

2. Go to System > PKI Servers.

3. Do one of the following:

   • Click New to add a new PKI server.

   • Select a PKI server already on the list and click Edit.

Use this page to configure connections to PKI Services Manager. Reflection PKI Services Manager provides certificate verification services, and is available as a separate download from the FileXpress Gateway download page at no additional charge. For information about downloading PKI Services Manager and configuring it for use with FileXpress Gateway, see Set Up PKI Services Manager (page 32).
<table>
<thead>
<tr>
<th><strong>PKI server</strong></th>
<th>The server running PKI Services Manager.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port</strong></td>
<td>The listening port used by PKI Services Manager. The default (18081) is the default port used by PKI Services Manager.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>New servers are enabled by default. Select <strong>Disabled</strong> to disable this PKI server without removing it from your list.</td>
</tr>
<tr>
<td><strong>Retrieve Public Key</strong></td>
<td>Retrieves the public key from the specified PKI server. After you retrieve a key, information about that key is displayed below the button. To compare the retrieved key fingerprint with the actual PKI Services Manager key on the PKI server, start the PKI Services Manager console and go to <strong>Utility &gt; View Public Key</strong>.</td>
</tr>
</tbody>
</table>
FileXpress Gateway System Administration

In this Section

- Configuring Email Messages in FileXpress Gateway 67
- Configuring the File Storage Server 73
- Server Certificate Management 77
- Configuration and Data Files 88
- Managing the FileXpress Gateway Services 94
- Ensuring High Availability of the FileXpress Gateway Servers 98
- Set Up File Transfer Auditing 108
- Change the JRE 109
- Customize the Look of the Transfer Client Web Pages 111
CHAPTER 7

Configuring Email Messages in FileXpress Gateway

FileXpress supports a number of optional email notification services. These include:

- Account creation email for new users
- Password reset email
- Transfer site access notification
- Notification sent to site managers and/or site members when files are uploaded or downloaded

Initial Email Setup

To support email services, you need to:

- Configure the Gateway Administrator Email Server (page 60) settings.
- Edit the Gateway Administrator container.properties (page 88) file to include the public-facing URL that will be used in email links.

For detailed procedures, see Configure Email Support in FileXpress Gateway Administrator (page 17).

Email Notifications

FileXpress Gateway supports the following email notifications.

<table>
<thead>
<tr>
<th>Notification</th>
<th>When is it sent?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account Creation</strong></td>
<td><strong>Account creation email is sent when:</strong></td>
</tr>
<tr>
<td>Provides a link for new users to set their password.</td>
<td>- Users are added using <strong>Users &gt; New</strong>, and <strong>Email registration</strong> is selected (the default).</td>
</tr>
<tr>
<td></td>
<td>- Users are added using <strong>Transfer Sites &gt; Quick Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Users are added using <strong>Transfer Site &gt; Add (or Edit) &gt; New FileXpress User</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Account creation email is not sent when:</strong></td>
</tr>
<tr>
<td></td>
<td>- Users are added using <strong>Users &gt; New</strong>, and <strong>Specify password</strong> is selected.</td>
</tr>
<tr>
<td></td>
<td>- Users are added by adding LDAP servers.</td>
</tr>
</tbody>
</table>
### Notification

<table>
<thead>
<tr>
<th>Notification</th>
<th>When is it sent?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transfer Site Access</strong></td>
<td>Sent by default to users who are added to a transfer site, either when it is first created or by edits to an existing site. You can enable or disable this notification for each site from the New/Edit Transfer Site page using Send email notification.</td>
</tr>
<tr>
<td><strong>File Upload</strong></td>
<td>Sent when a file is successfully uploaded to a transfer site. Upload notification is site-specific and is disabled by default. You can enable notifications for any member of a site from the New/Edit Transfer Site page. Click the icon under Notifications in the member list.</td>
</tr>
<tr>
<td><strong>File Download</strong></td>
<td>Sent when a file is successfully downloaded from a transfer site. Download notification is site-specific and is disabled by default. You can enable notifications for any member of a site from the New/Edit Transfer Site page. Click the icon under Notifications in the member list.</td>
</tr>
<tr>
<td><strong>Password Request</strong></td>
<td>Sent to users who click the Forgot password? link in the Transfer Client login page.</td>
</tr>
<tr>
<td><strong>Password Reset</strong></td>
<td>Sent to users who have successfully reset their password.</td>
</tr>
</tbody>
</table>

#### Customize Email Templates

You can customize the content and/or format of the email messages sent from FileXpress Gateway Administrator. Your customized content can use either text or HTML format.
Before you begin

- Configure Email Support in FileXpress Gateway Administrator (page 17).

To customize an email template

1. Log on to Gateway Administrator using an account in the Administrators group (or any account that has the System setup role enabled).

2. Go to System > Email templates.

3. Select the template you want to customize. (Account Creation is displayed by default.)

4. Select the user pool (FileXpress users or users in an added LDAP server) for this template.

   Note the following:
   - If you want to send the same customized email to both user pools, customize the template for each pool in a separate step.
   - Account Creation and Password Reset are not available for LDAP users.

5. (Optional) Customize the Sender address, Sender name, and Subject for this email. The default tokens entered for address and name are replaced with the global values specified in the Email Server tab. You can delete these tokens and replace them with an actual address or sender name.

6. Edit the message text using any combination of the following techniques. The text can use either text or HTML format.

   - Edit the text directly in Gateway Administrator. Click Insert token to insert a token (page 70) in the current cursor position. This automatically inserts the token with the required dollar signs ($).

   - Click Import to import content you have created and saved using a text or HTML editor. To add tokens in these editors, type the token name manually, including the required dollar signs.

   - Copy and paste text into the message body.

7. (Optional) Expand the Preview feature to preview your email or send a test email. Note the following:

   - Tokens in the preview are replaced by sample content enclosed in square brackets. For example: [myTransferSite]. In actual generated email, the brackets do not appear and the sample content is replaced by actual content.

   - To send a test email, enter an email address and click Send Test Email. This test can help you determine if your email server is correctly configured and supports your current values for Sender address and Sender name.

8. Click Save.

9. (Recommended) Because the preview email messages do not show how token replacement is actually handled, you should follow up a successful preview test with a test of an actual email notification.

Sample HTML content

The following example shows a sample HTML alternative to the Transfer Site Access email.
Email Tokens

Email messages support the use of tokens. Tokens included in email templates are replaced by actual values in the generated email.

- Tokens must preceded and followed by a dollar sign ($), for example $TIME$.
- You can type tokens into a message manually or select a token from the Insert token list. The token list shows which tokens are supported for each template type.
- Tokens for which no value is available are omitted from email messages.
- You can use the Preview feature on the Email Templates tab to see sample output. To see actual replacement values, send a test email.

The following tokens are supported:

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
<th>Available with</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCOUNT_EXPIRATION_DATE</td>
<td>The account expiration date of the user receiving the email.</td>
<td>All</td>
</tr>
<tr>
<td>CLIENT_IP</td>
<td>The IP address of the client system.</td>
<td>File Upload File Download</td>
</tr>
<tr>
<td>CUSTOM_MESSAGE</td>
<td>Custom message from New/Edit Transfer Site. If no custom message is configured, this token is replaced by an empty string.</td>
<td>Transfer Site Access File Upload File Download</td>
</tr>
<tr>
<td>DATE</td>
<td>The date of the action.</td>
<td>All</td>
</tr>
<tr>
<td>FILENAME</td>
<td>The name of the uploaded or downloaded file.</td>
<td>File Upload File Download</td>
</tr>
<tr>
<td>FILE_HASH</td>
<td>The SHA-1 hash of the uploaded or downloaded file.</td>
<td>File Upload File Download</td>
</tr>
<tr>
<td>FILE_PATH</td>
<td>The path—without the filename—to the destination directory (uploads) or source directory (downloads) on the file storage server.</td>
<td>File Upload File Download</td>
</tr>
<tr>
<td>FILE_SIZE</td>
<td>The file size (in bytes).</td>
<td>File Upload File Download</td>
</tr>
<tr>
<td>Token</td>
<td>Description</td>
<td>Available with</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>FIRST_NAME</td>
<td>The first name of the user receiving the email.</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>Note: First name is an optional field for FileXpress users. If no first name is available, this token is replaced by an empty string.</td>
<td></td>
</tr>
<tr>
<td>FULL_PATH</td>
<td>The path—including the filename—to the destination file (uploads) or source file (downloads) on the file storage server.</td>
<td>File Upload File Download</td>
</tr>
<tr>
<td>GLOBAL_SENDER_ADDRESS</td>
<td>Sender address from Email Server.</td>
<td>All</td>
</tr>
<tr>
<td>GLOBAL_SENDER_NAME</td>
<td>Sender name from Email Server.</td>
<td>All</td>
</tr>
<tr>
<td>INITIATOR_EMAIL</td>
<td>The email of the action initiator (defined below)</td>
<td>All</td>
</tr>
<tr>
<td>INITIATOR_USERID</td>
<td>The user ID of the action initiator (defined below). For LDAP users, the domain name is included (domain\userID). For FileXpress users, the domain name is omitted (userID).</td>
<td>All</td>
</tr>
<tr>
<td>LAST_NAME</td>
<td>The last name of the user receiving the email.</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>Note: Last name is an optional field for FileXpress users. If no last name is available, this token is replaced by an empty string.</td>
<td></td>
</tr>
<tr>
<td>PASSWORD_RESET_LINK</td>
<td>The URL that links to the password reset page.</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>The host and port are set in the Gateway Administrator properties file using the transfer.server.url.</td>
<td></td>
</tr>
<tr>
<td>PASSWORD_RESET_LINK_TIMEOUT</td>
<td>The length of time password reset can be accomplished after a reset email is sent. This value is configured in the Gateway Administrator properties file using password.reset.expiration.</td>
<td>All</td>
</tr>
<tr>
<td>TIME</td>
<td>For uploads and downloads, this is the time on the FileXpress Secure Shell Proxy. For all other events, this is the time on the Gateway Administrator.</td>
<td>All</td>
</tr>
<tr>
<td>TIMEZONE</td>
<td>The time zone of the FileXpress Gateway Administrator.</td>
<td>All</td>
</tr>
<tr>
<td>TRANSFER_SITE_DESCRIPTION</td>
<td>Description from New/Edit Transfer Site.</td>
<td>Transfer Site Access File Upload File Download</td>
</tr>
<tr>
<td></td>
<td>Note: Description is an optional field. If no description is available, this token is replaced by an empty string.</td>
<td></td>
</tr>
<tr>
<td>Token</td>
<td>Description</td>
<td>Available with</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>TRANSFER_SITE_LINK</td>
<td>The URL for connecting to the Transfer Client. The host and port are set in the Gateway Administrator properties file using the transfer.server.url.</td>
<td>Transfer Site Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>File Upload</td>
</tr>
<tr>
<td>TRANSFER_SITE</td>
<td>The Transfer site name from New/Edit Transfer Site.</td>
<td>Transfer Site Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>File Upload</td>
</tr>
<tr>
<td></td>
<td></td>
<td>File Download</td>
</tr>
<tr>
<td>USERID</td>
<td>The User ID of the user receiving the email.</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>For LDAP users, the domain name is included: domain\userID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For FileXpress users the domain name is omitted: userID.</td>
<td></td>
</tr>
<tr>
<td>USER_EMAIL</td>
<td>The email address of the user receiving the email.</td>
<td>All</td>
</tr>
</tbody>
</table>

**Action Initiator**

Some email tokens include information about the action initiator, as indicated in the table above. The action initiator depends on which template is in use:

**In this template:**  **The action initiator is:**

<table>
<thead>
<tr>
<th>In this template:</th>
<th>The action initiator is:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Creation</td>
<td>User who added the account to the FileXpress Users list</td>
</tr>
<tr>
<td>Transfer Site Access</td>
<td>User who added the recipient to the transfer site</td>
</tr>
<tr>
<td>File Upload</td>
<td>User who uploaded the file</td>
</tr>
<tr>
<td>File Download</td>
<td>User who downloaded the file</td>
</tr>
<tr>
<td>Password Request</td>
<td>User who clicked the &quot;Forgot password?&quot; link</td>
</tr>
<tr>
<td>Password Reset</td>
<td>User who clicked the &quot;Forgot password?&quot; link</td>
</tr>
</tbody>
</table>
CHAPTER 8

Configuring the File Storage Server

In this Chapter

Configure File Storage on the FileXpress Proxy 73
Configure File Storage on an SFTP Server 74
Configure Additional SFTP Servers Using the FileXpress Secure Shell Proxy 74

Transfer site directories are created within a base directory on a designated file storage server. The procedures in this section describe how to designate the file storage server and specify which directory is used as the base directory on that server.

Configure File Storage on the FileXpress Proxy

The file storage server setting is configured in Gateway Administrator under System > File Storage. By default, FileXpress Gateway creates transfer site directories on the FileXpress Gateway Proxy.

- The default base directory on the FileXpress Gateway Proxy is configured using the FileXpress Secure Shell Proxy console, not using Gateway Administrator. This can be a local folder on the FileXpress Secure Shell Proxy computer or an accessible network share.

- The name and location of the base directory you configure for your file storage server is not made visible to client users. The folder name that users see when they connect is the value you specify for Transfer site name when you create a transfer site. The actual subdirectory on the file storage server is the value you specify for Directory name.

The default base directory on the FileXpress Gateway Proxy is:

C: \ProgramData\Attachmate\RSecureServer\FileXpress\n
To modify the base directory on the FileXpress Gateway Proxy

1. Start the FileXpress Secure Shell Proxy console. It is installed in the Windows Start menu (or Apps list) under Attachmate FileXpress Gateway > FileXpress Secure Shell Proxy.


Note: You can specify a local path, a mapped drive, or a UNC path. If you specify a network location, set FileXpress user access account to a user who has access to that location.

3. Save your settings (File > Save Settings).
Configure File Storage on an SFTP Server

You can use the following procedure to configure file storage on any SFTP server. Typically this will be a server running in your internal network. This is the recommended configuration when the FileXpress Gateway Proxy is running in the DMZ. With this configuration, data streams continuously through the proxy, eliminating the need to save files on this server. Data passed to the SFTP server is securely encrypted.

Before you begin

- Install the Reflection for Secure IT Server (page 11) on the system you want to use for file storage.
  
  - or -

  Designate an existing SFTP server available in your network to use for file storage.

- Obtain the name or IP address of the SFTP server, and obtain valid user credentials for logging on to this server.

To configure file storage on an SFTP server

1. Log on to Gateway Administrator using an account in the Administrators group (or any account that has the System setup role enabled).
2. Go to System > File Storage and select SFTP server.
3. Enter values for Server and Port.
   - Click Retrieve to retrieve the host key for this server.
   - For UserID and Password, enter valid credentials on this server.
   - For Base directory, click Browse and select a location available to this user. By default, the base directory is set to a subdirectory called FileXpressGateway in the directory you select. This is not required; you can edit or delete this subdirectory name.

Note: The name and location of the base directory you configure for your file storage server is not made visible to client users. The folder name that users see when they connect is the value you specify for Transfer site name when you create a transfer site. The actual subdirectory on the file storage server is the value you specify for Directory name.

4. Click Save.

Configure Additional SFTP Servers Using the FileXpress Secure Shell Proxy

The File Storage setting in FileXpress Gateway Administrator allows you to specify a single SFTP server for file storage. Any transfer site you define using Gateway Administrator uses a directory on this server. This option is easy to use and configure, and is the recommended configuration.

It is also possible to configure directory access on additional servers using the SFTP Directories feature of the FileXpress Secure Shell Proxy; however, directories made available this way are managed differently from transfer sites. Review the following limits and differences before you proceed.
Directories configured this way will not have access to transfer site features added in future releases.

To transfer files using the FileXpress Transfer Client, users must have access to at least one transfer site configured using the Gateway Administrator. Users who have no transfer sites will see a message saying that no transfer sites are available, even if they have access to one or more SFTP directories configured using the FileXpress Secure Shell Proxy. Use one of the following approaches to work around this limitation:

Ensure that all users have at least one transfer site configured in Gateway Administrator.

-OR-

Direct users to connect directly to the FileXpress Secure Shell proxy using an alternate SFTP client, such as the Reflection FTP Client, instead of using the FileXpress Transfer Client. These users should connect using the listening port configured on the Network pane of the FileXpress Secure Shell Proxy (22 by default). Users connecting this way will see shared SFTP directories configured using the FileXpress Secure Shell Proxy, as well as transfer sites created using Gateway Administrator.

To control who has access to a transfer site created using Gateway Administrator, you add or remove users and groups on the Transfer Site page. To control who has access to an SFTP directory configured in the FileXpress Secure Shell Proxy, you use the Subconfiguration feature.

The following procedure configures a shared directory on an SFTP server that will be available to all users.

**To configure a connection to an SFTP server from the FileXpress Secure Shell Proxy**

1. Start the FileXpress Secure Shell Proxy console. It is installed in the Windows Start menu (or Apps list) under Attachmate FileXpress Gateway > FileXpress Secure Shell Proxy.

2. From the Configuration tab, click SFTP Directories in the left panel, then click Add. This opens the Accessible Directory Settings dialog box.

3. Enter a Virtual directory name. This is the folder name that will be visible to users.

4. Select Remote SFTP server. This opens the Remote SFTP Server Connection dialog box.
   - For Host, specify the name or IP address of the SFTP server.
   - Click Retrieve to retrieve the public key used to authenticate this server.
   - For Remote SFTP username and Password, enter the credentials of the user account that will provide access to the file system on the remote SFTP server.
   - Under Remote base directory, click Browse to select the directory you want to make available to users. This must be a directory accessible to the user you entered for Remote SFTP username.

5. Click Test Connection. You should see a message saying that the connection was successful.

6. Click OK to close the dialog boxes and return to the SFTP Directories pane.

---

Note: The User login directory option, including the default /Home directory, is not used for FileXpress users.
Use the next procedure to limit access to a directory on an SFTP server to members of a FileXpress group or to an individual FileXpress user.

**To configure directory access for a FileXpress group or user**

1. From the FileXpress Secure Shell Proxy console **Configuration** tab, under **Subconfiguration** click either **User Configuration** or **Group Configuration**.
2. Click **Add**.
3. Click **Domain** (for user configuration) or set **Group type** to **Domain** (for group configuration).
   - For members of the FileXpress LDAP server, set the domain name to **FileXpress**.
   - For members of an added LDAP server, use the **Domain name** as it appears on the **LDAP Servers** page in Gateway Administrator.
4. Enter the name of the user or group your are configuring.
5. In the left portion of the **Group Configuration** dialog box, click **SFTP Directories**.
6. Clear the **Inherit directories** check box.
7. Click **Add** to open the **Accessible Directory Settings** dialog box.
8. Configure the remote directory that will be available to this user or group, as described in the preceding procedure, starting with step 3.
When users log on to Gateway Administrator or the FileXpress Transfer Client, the connection is made using HTTPS and the browser requires server authentication. By default, the FileXpress servers send a self-signed security certificate to the browser for this purpose. (A self-signed certificate is signed by the same entity that it certifies.) The browser checks the digital signature in this certificate against its list of trusted Certificate Authorities (CAs). With the default certificates, you see a certificate warning, because the signer of the certificate is not in your browser’s list of trusted CAs.

The procedures in this section describe options for managing these server certificates.

**Replace the Default Server Certificate**

The following two FileXpress Gateway services install with self-signed digital certificates.

- Attachmate FileXpress Transfer Server
- Attachmate FileXpress Gateway Administrator

To be able to connect to the Transfer Client and Gateway Administrator without seeing certificate warning messages, you can replace each of these self-signed certificates with a certificate from a well-known Certificate Authority (CA). Server certificates can be stored in a PKCS#12 file (*.p12 or *.pfx) or in a Java keystore (*.jks). Refer to the following procedures for details.

Install a Server Certificate in a PKCS#12 File (page 77)

Install a Server Certificate in a Java Keystore (page 79)

**Install a New Server Certificate: PKCS#12 File**

Use this procedure to replace the default Transfer Server or Gateway Administrator server certificate with a CA-signed certificate contained within a PKCS#12 file.

**Before you begin**

Obtain a PKCS#12 file (*.p12 or *.pfx) that includes your private key and a certificate signed by a Certificate Authority (CA).
Notes:

- Both the private key in the keystore and the keystore itself must use FIPS-compliant cryptography. You should request a FIPS-compliant key from your Certificate Authority. PBE-SHA1-3DES is the only approved algorithm currently available for encrypting the store. (By default, OpenSSL and the Windows Certificate Manager do not encrypt the store using this algorithm.) If you have a PKCS#12 file that has a FIPS-compliant private key, but the store encryption is not FIPS-compliant, you can re-encrypt the PKCS#12 file (page 86) or import the file into a Java keystore (page 86).
- The PKCS#12 store and the private key must be protected with the same password.

---

To replace the default server certificate with a certificate in a PKCS#12 file (*.p12 or *.pfx)

1. Move the PKCS#12 file to the folder that holds the default FileXpress keystore (or to any secure location on your server). The default keystore locations are:

   `<install path>\TransferServer\etc`

   `<install path>\GatewayAdministrator\etc`

Caution: Do not delete any of the existing certificates or keystore files in these locations. The server certificates located here are required for communication between FileXpress Gateway components.

2. Locate the `container.properties` file in the location below for the server you are updating.

   `<install path>\TransferServer\conf\container.properties`

   `<install path>\GatewayAdministrator\conf\container.properties`

3. Open `container.properties` in a text editor (running as an administrator). Remove the comment character (#) from the following lines. Set `servletengine.ssl.keystoretype` to PKCS12 and edit `servletengine.ssl.keystore` and `servletengine.ssl.keystorepassword` to use your values. For example:

   `servletengine.ssl.keystore=../etc/myserver_cert.p12`

   `servletengine.ssl.keystoretype=PKCS12`

   `servletengine.ssl.keystorepassword=mypassword`

Note: The path to the keystore must be specified using either forward slashes or escaped backslashes. For example: `C:/path/to/keystore` or `C:\path\to\keystore`

4. Restart the server you are configuring. See Start and Stop the FileXpress Transfer Server (page 94) and Start and Stop the FileXpress Gateway Administrator Service (page 94).

5. If you replaced the Gateway Administrator certificate, you must repeat the **Activate and verify** (page 15) action on the FileXpress Secure Shell Proxy. This reestablishes the connection to the Gateway Administrator using the new certificate.
6 Confirm that you can log on to the Transfer Client or Gateway Administrator.

   If you can't log in, or if you continue to see a certificate warning message, see Troubleshooting Server Certificate Setup (page 122).

**Install a New Server Certificate: Java Keystore**

Use this procedure to replace the default Transfer Server or Gateway Administrator server certificate with a CA-signed certificate contained within a Java keystore.

**Before you begin**

Obtain a Java keystore (*.jks) file that contains your private key and a certificate signed by a Certificate Authority (CA). You can use the following procedures to create your keystore using the Java `keytool` utility.

- Generate a key pair and create a keystore (page 83).
- Create a Certificate Signing Request and submit it to a CA (page 84).
- Import the CA-signed certificate into your keystore (page 85).

**To replace the default server certificate with a certificate in a Java keystore**

1 Move the new Java keystore to the folder that holds the default keystore (or to any secure location on your server). The default keystore locations are:

   `<install path>\TransferServer\etc\`

   `<install path>\GatewayAdministrator\etc\`

   **Caution:** Do not delete any of the existing certificates or keystore files in these locations. The server certificates located here are required for communication between FileXpress Gateway components.

2 Locate the `container.properties` file in the location below for the server you are updating.

   `<install path>\TransferServer\conf\container.properties`

   `<install path>\GatewayAdministrator\conf\container.properties`

3 Open `container.properties` in a text editor (running as an administrator). Remove the comment character (#) from the following lines and edit them to point to your keystore and specify your keystore password. For example:

   `servletengine.ssl.keystore=../etc/newkeystore.jks`

   `servletengine.ssl.keystorepassword=mypassword`

   **Note:** The path to the keystore must be specified using forward slashes or escaped backslashes. For example: `C:/path/to/keystore` or `C:\path\to\keystore`
4  Restart the server you are configuring. See Start and Stop the FileXpress Transfer Server (page 94) and Start and Stop the FileXpress Gateway Administrator Service (page 94).

5  If you replaced the Gateway Administrator certificate, you must repeat the Activate and verify (page 15) action on the FileXpress Secure Shell Proxy. This reestablishes the connection to the Gateway Administrator using the new certificate.

6  Confirm that you can log on to the Transfer Client or Gateway Administrator. If you can't log in, or if you continue to see a certificate warning message, see Troubleshooting Server Certificate Setup (page 122).

Configure Your Browser to Trust a Self-Signed Certificate

If you use the default FileXpress Gateway certificates, you will see a certificate warning when you connect to the Gateway Administrator and the Transfer Client. Use these procedures to remove these warnings.

Note: The procedures below are appropriate for testing. However, before you deploy the Transfer Client to end users, you should configure FileXpress Gateway to use certificates signed by a well-known Certificate Authority. (See Replace the Default Server Certificate (page 77).) With the updated certificate in place, the following procedures are not necessary.

To add an untrusted certificate in Internet Explorer

1  When you see a warning that the security certificate was not issued by a trusted certificate authority, select Continue to this website.

   This connects you to the web page and displays a certificate error alert in the address bar.

2  Click the certificate error alert to view the Certificate Error message shown here:
3 Click View Certificates.

4 On the certificate General tab, click Install Certificate.

Note: If the Install Certificate button is not visible, you need to modify your browser's security settings. Go to Tools > Internet Options > Security, then clear Enable Protected Mode. You can restore this setting after you install the certificate.

5 In the Install Certificate Wizard, select Place all certificates in the following store.

6 Click Browse and select Trusted Root Certification Authorities, then continue through the remaining steps to install the certificate.

Note: Chrome uses the same certificate store as Internet Explorer, so adding a certificate here also adds it for Chrome.

To add an untrusted certificate in Firefox

1 When you see a warning that the connection is untrusted, click I understand the Risks.

2 Click Add Exception.

3 Leave Permanently store this exception selected and click Confirm Security Exception.

4 Click OK to close the dialog boxes.

To add an untrusted certificate in Chrome

1 The certificate warning message you see depends on your Chrome version:

   • If you see a message that says your connection is not private, click Advanced, then click the Proceed to link.

   • If you see a message that says the site's security certificate is not trusted, click Proceed anyway.

2 Save the presented certificate to a file. To do this:

   • Click the site information icon in the address bar:

   • Click Certificate Information.

   • On the Details tab, click Copy to File and save the file using defaults.

3 Open the Windows certificate store:

   • Click the customize button (three bars) in the upper right:

   • Click Settings.

   • Click Show advanced settings.

   • Click Manage certificates.
4 Import the saved certificate:
   • Click the **Trusted Root Certification Authorities** tab.
   • Click **Import**, then continue through the remaining steps to install the certificate.

**To add an untrusted certificate in Safari**

1 When you see a warning that Safari can't verify the identity of the website, click **Show Certificate**.
2 Click the arrow next to **Trust** to view the options.
3 Select **Always Trust** in the drop-down list for the option **When using this certificate**.
4 Click **Continue**.
5 Enter your password to modify your Certificate Trust settings.

**Using the Keytool Utility to Manage Keystores**

The Java `keytool` utility is a command-line tool that can be used to manage keys and certificates. Depending on how you obtain certificates, you can use one or more of these procedures to manage your FileXpress Gateway certificates. For more complete documentation, refer to the `keytool` documentation (http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html).

Run the Keytool Utility

Generate a Key Pair and Create a Keystore
Create and Submit a Certificate Signing Request
Import Certificates from a p7b package into your Java Keystore
Import Individual Certificates into your Keystore
Import a PKCS#12 File into a Java Keystore
Re-encrypt a PKCS#12 file to Use Stronger Encryption

**Run the Keytool Utility**

The `keytool` utility is a key and certificate management tool that is installed with the Java JRE.

**To run the keytool utility**

1 Open a Command Prompt window running as an administrator. *(Start > All Programs > Accessories, right-click Command Prompt > Run as administrator.)*
2 Navigate to the folder that contains keytool.exe or add this folder to your path. (Confirm the actual ServerJDK version for your installation.) For example:

```plaintext
SET PATH=%PATH%;C:\Program Files\Common Files\Attachmate\ServerJDK\1.7.0_75\bin
```

3 To review the available options, enter the following:

```plaintext
keytool -help
```

## Generate a Key Pair and Create a Keystore

This procedure uses the Java `keytool` (page 82) utility to generate a key and save it to a Java keystore.

---

Note: The CA you use might have specific options required for creating an HTTPS certificate. Review the instructions provided by the CA before creating your key pair.

---

### To generate a new public/private key pair in a Java keystore

1 Use the `-genkeypair` option to generate a key and save it to a Java keystore (`newkeystore.jks` in this example). The example shown here prompts you to enter values for items that make up the distinguished name (DN) in the certificate. See the example below to enter these values directly on the command line.

```plaintext
keytool -genkeypair -alias filexpress -keyalg RSA -keysize 2048 -keystore newkeystore.jks -validity 365 -storetype JCEKS
```

2 The `keytool` prompts you to enter a password and values for the items that make up the distinguished name (DN) in the certificate (name = CN, organizational unit = OU, organization = O, city or locality = L, state or province = S, two letter country code = C). The generated DN will use the value "Unknown" for any fields you don’t specify.

- When you are prompted with “What is your first and last name?”

  You must enter the DNS name that is used to access the FileXpress Gateway server (for example filexpress.mycompany.com). This value is used as the CN (Common Name) in the certificate. If the CN in a certificate doesn't match the actual DNS name used to access the server, you will see a certificate warning when you connect to the server.

- When you are prompted with "What is the two-letter country code for this unit?"

  You must enter a valid two-letter country code (for example US).

3 When you are prompted for a password for the alias, press Enter to use the same password you used for the keystore.

An alternate option to responding to prompts is to specify the DN value on the command line using the `-dname` option. For example:

```plaintext
```
Create and Submit a Certificate Signing Request

This procedure uses the Java keytool (page 82) utility to create a Certificate Signing Request (CSR) from an existing keystore.

Before you begin

- You need to know the keystore name, password, and alias you used when you created the keystore (page 83).

To create and submit a Certificate Signing Request

1. Use the -certreq option to generate a certificate request. This generates a Certificate Signing Request, using the PKCS#10 format. For example:

   ```bash
   keytool -v -certreq -alias filexpress -keystore newkeystore.jks -file cert_request.csr -ext ExtendedkeyUsage=serverAuth -storetype JCEKS
   ```

2. Enter your keystore password when prompted.

3. You will see a message saying that the certificate request has been saved to the file you specified (cert_request.csr in this example).

4. Submit this CSR to your CA. You will need the contents of the CSR file. Open the file in a text editor. The contents should include a header and footer with encoded data between them. When you submit the request, copy the entire file, including the BEGIN and END lines.

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   <encoded data>
   -----END CERTIFICATE REQUEST-----
   ```

Import Certificates from a p7b package into your Java Keystore

Typically the Certification Authority will provide you with a PKCS#7 package (*.p7b) that contains the full chain of certificates required to authenticate your server (the CA-signed server certificate, intermediate certificates, and the CA root certificate). This procedure uses Java keytool (page 82) command to import the certificates from the p7b file into your Java keystore.

Note: If you have individual certificates not contained within a p7b package do not use this procedure. You will need to import each certificate separately. See the procedure described in Import Individual Certificates into your Keystore (page 85).

Before you begin

- Obtain a PKCS#7 package (*.p7b) from the Certification Authority that contains the CA-signed server certificate, intermediate certificates, and the CA root certificate.

- You need to know the keystore name, password, and alias you used when you created the keystore (page 83).
To import certificates contained within a p7b file

- Add the certificates from the PKCS #7 file (FullChainOfCerts.p7b in this example) to the Java keystore. The alias in this command needs to match the alias you specified when you generated your key pair. For example:

  ```
  keytool -importcert -alias filexpress -trustcacerts -file FullChainOfCerts.p7b -keystore newkeystore.jks –storetype JCEKS
  ```

Import Individual Certificates into your Keystore

Use this procedure if certificates (the CA-signed server certificate, intermediate certificates, and the CA root certificate) are obtained as individual certificates instead of in a single PKCS#7 (*.p7b) file. This procedure uses a series of Java keytool (page 82) commands to import these certificates into an existing keystore. Use the order of import as shown in the procedure: import the root CA first, then any required intermediate certificates, and finally, the CA-signed server certificate.

Note: If your certificate was provided within a p7b package, you do not need to import each certificate separately. Instead, use the procedure described in Import Certificates from a p7b package into your Java Keystore (page 84).

Before you begin

- Obtain a server certificate for your server signed by a Certificate Authority.
- Obtain the trusted root CA certificate for the Certificate Authority and any required intermediate certificates.
- You need to know the keystore name, password, and alias you used when you created the keystore (page 83).

To import certificates into your Java keystore

1. Add the root CA certificate (CAcert.cer in this example) to the Java keystore that you generated when you created your private key (newkeystore.jks in this example). Use a new alias (root in this example). For example:

   ```
   keytool -importcert -alias root -file CAcert.cer -keystore newkeystore.jks –storetype JCEKS
   ```

2. Add each required intermediate certificate (IntermediateCAcert.cer in this example) to the Java keystore:

   ```
   keytool -importcert -alias intermediate -trustcacerts -file IntermediateCAcert.cer -keystore newkeystore.jks –storetype JCEKS
   ```

3. Add the CA-signed server certificate (EndEntitycert.cer in this example) to the Java keystore. The alias in this command needs to match the alias you specified when you generated your key pair. For example:

   ```
   keytool -importcert -alias filexpress -trustcacerts -file EndEntitycert.cer -keystore newkeystore.jks –storetype JCEKS
   ```
Import a PKCS#12 File into a Java Keystore

This procedure uses the Java keytool (page 82) utility to create a Java keystore from a PKCS#12 file.

Before you begin

- You need a PKCS#12 (*.p12 or *.pfx) file containing your CA-signed FileXpress Gateway server certificate and private key.
- You need to know the password that protects this file.

To import a PKCS#12 file into a Java keystore

1. Use the -importkeystore option to create a Java keystore (newkeystore.jks in this example). For example:

   ```
   keytool -importkeystore -v -srckeystore cert_file.p12 -srcstoretype PKCS12 -destkeystore newkeystore.jks -deststoretype JCEKS
   ```

   **Note:** The keystore type you specify for deststoretype must match the type specified for servletengine.ssl.keystoretype in the server's container.properties file. JCEKS is specified by default, and is recommended because it uses a stronger encryption for protecting the private key.

2. Enter passwords when prompted using the same password for destination keystore and source keystore.

   **Note:** If these passwords don't match, the server will not be able to use the Java keystore and the browser will not be able to launch the application.

Re-encrypt a PKCS#12 file to Use Stronger Encryption

If you configure a FileXpress server to authenticate with a PKCS#12 file, the file must be encrypted with a FIPS-approved algorithm. If the encryption is too weak, your browser will not be able to connect to the service and the console log file will include a message saying "java.io.IOException: Could not decrypt data." You can use the keytool utility to re-encrypt your package.

To re-encrypt a PKCS#12 file using a FIPS-approved algorithm

1. Open a Command Prompt window running as an administrator. (Start > All Programs > Accessories, right-click Command Prompt > Run as administrator.)

2. Use a SET command to add the keytool folder to your path. (Confirm the actual ServerJDK version for your installation.) For example:

   ```
   SET PATH=%PATH%;C:\Program Files\Common Files\Attachmate\ServerJDK\1.7.0_75\bin
   ```
3 Define a variable called `FXG_ROOT` that points to your FileXpress installation folder. For example:

```
SET FXG_ROOT=C:\Program Files\Attachmate\FileXpress\Gateway
```

4 Run the following command, replacing `nonfips.p12` and `fips.p12` with your source and destination filenames. (This is a single-line command. Hyphens shown here are all required characters. Ensure that there are no spaces after hyphens and semicolons.)

```
keytool -providerName JsafeJCE -providerClass com.rsa.jsafe.provider.JsafeJCE -providerPath "%FXG_ROOT%\TransferServer\lib\cryptojce-6.1.2.jar;%FXG_ROOT%\TransferServer\lib\cryptojcommon-6.1.2.jar;%FXG_ROOT%\TransferServer\lib\jcmFIPS-6.1.2.jar" -importkeystore -srckeystore nonfips.p12 -destkeystore fips.p12 -deststoretype PKCS12 -srcstoretype PKCS12
```

5 Enter passwords when prompted using the same password for destination keystore and source keystore.

---

**Note:** If these passwords don't match, the server will not be able to use the keystore and the browser will not be able to launch the application.
Chapter 10

Configuration and Data Files

In this Chapter

- Gateway Administrator Properties File 88
- FileXpress Transfer Server Properties File 90
- FileXpress Gateway Data Files 91
- Backing Up Gateway Administrator Data 93

Gateway Administrator Properties File

You can use the Gateway Administrator properties file to modify the configurable settings listed below. It is located in the FileXpress Gateway installation folder in the \GatewayAdministrator\conf subfolder. The default location is:

C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\conf

Notes:

- You must restart the server (page 94) after editing container.properties for your changes to take effect.
- A backup file, container.properties.example, in the same folder provides a copy of the original default settings.

rmi.port.ssl

The ssl-enabled port used to configure clustering. The ConfigServer (page 104) command line utility uses this port to communicate to Gateway Administrators when you add instances to a cluster, remove instances from a cluster, or list instances a cluster. This is disabled (0) by default. Set this value to 43000 to support a Gateway Administrator cluster. If you specify a number other than 43000, the port number must be specified in the ConfigServer command line.

replication.enabled

Specifies whether data replication is supported between multiple instances of a Gateway Administrator cluster (page 99). Allowed values are true or false. The default is false.

directory.replication.port

The port used for data replication between members of a Gateway Administrator cluster. This setting must be the same across all instances of Gateway Administrator within the cluster. The default is 8846.
ldaps.port.enabled

Set this option to true to expose the internal Gateway Administrator LDAP server. The default is false.

directory.ldaps.port

Specifies the listening port used by the Gateway Administrator LDAP server when ldaps.port.enabled is true.

servletengine.ssl.port

The HTTPS port used to connect to the Gateway Administrator. The default is 9490.

transfer.server.url

The public-facing base URL of the FileXpress Transfer Server. This is used in URLs included in email messages sent from Gateway Administrator.

password.reset.expiration

Sets the token expiration time (in minutes) for password reset. Users who request a password recovery email must perform the reset before the token expires.

configservice-ws.host

Specifies the hostname or IP address that the Gateway Administrator web service listens on. The FileXpress Secure Shell Proxy and the FileXpress Transfer Server communicate with this web service. If no host is specified (the default), the Gateway Administrator listens on all available IP addresses on the Gateway Administrator server.

configservice-ws.port

Specifies the port that the Gateway Administrator web service listens on. This value must match the value configured on the FileXpress Secure Shell Proxy (set from console using FileXpress Users > Gateway Administrator port) and for the Transfer Server (set by clicking Activate and verify in the FileXpress Users pane, which automatically updates configservice-ws.port in the Transfer Server properties file). The default is 9190.

servletengine.ssl.keystore

The path to the keystore that contains the server certificate and private key. For more information about changing the server certificate, see Replace the Default Server Certificate (page 77). The path must be specified using forward slashes or escaped backslashes. For example:

C:/path/to/keystore

C:\path\to\keystore

You can specify a relative or absolute path. The default is ../etc/mycert.jks.

servletengine.ssl.keystoretype

The file type of the keystore that contains the server certificate and private key. Supported values are JCEKS for a Java keystore, and PKCS12 for a PKCS#12 file. The default is JCEKS.

servletengine.ssl.keystorepassword

The password that protects the keystore that contains the server certificate and private key.
configservice.email.threads

Specifies the number of emails to process in parallel. If the number of active emails is under this limit, the email will be processed immediately; otherwise, it will wait its turn in the queue. The default is 10.

configservice.event.threads

Specifies the number of post transfer action events to process in parallel. If the number of active events is under this limit, the action will start immediately; otherwise, it will wait its turn in the queue. The default is 10.

configservice.account.expiration

The default number of days after which a newly created FileXpress user account expires. The default is 730 (two years). Set this to 0 (zero) to default to no expiration date.

configservice.transfersite.expiration

The default number of days after which a newly created FileXpress transfer site expires. The default is 730 (two years). Set this to 0 (zero) to default to no expiration date.

FileXpress Transfer Server Properties File

You can use the FileXpress Transfer Server properties file to modify the configurable settings listed below. It is located in the FileXpress Gateway installation folder in the TransferServer\conf subfolder. The default location is:

C:\Program Files\Attachmate\FileXpress\Gateway\TransferServer\conf

Notes:

- You must restart the server (page 94) after editing container.properties for your changes to take effect.
- A backup file, container.properties.example, in the same folder provides a copy of the original default settings.

servletengine.ssl.port

The HTTPS port used to connect to the Transfer Client. The default is 9492.

servletengine.ssl.updateInterval

The interval in seconds for how often the Transfer Server checks for changes to authentication settings made in Gateway Administrator and queries Gateway Administrator for PKI Services Manager trust anchors. The default is 60.

servletengine.ssl.keystore

The path to the keystore that contains the server certificate and private key. For more information about changing the server certificate, see Replace the Default Server Certificate (page 77). The path must be specified using forward slashes or escaped backslashes. For example:

C:/path/to/keystore
C:\path\to\keystore

You can specify a relative or absolute path. The default is ../etc/mycert.jks.

**servletengine.ssl.keystoretype**

The file type of the keystore that contains the server certificate and private key. Supported values are **JCEKS** for a Java keystore, and **PKCS12** for a PKCS#12 file. The default is **JCEKS**.

**servletengine.ssl.keystorepassword**

The password that protects the keystore that contains the server certificate and private key.

**sftp.hostname**

The hostname used by the Transfer Server to connect to the FileXpress Secure Shell Proxy Server. By default, the connection is made using the FileXpress Secure Shell Proxy Server’s computer name.

**sftp.port**

The port used by the Transfer Server to connect to the FileXpress Secure Shell Proxy Server. The default is 22.

---

**FileXpress Gateway Data Files**

Caution: The data locations below contain sensitive information. Windows administrator privileges are required in order to read or write to these file locations. You should not change these permissions. Any new locations you copy the files to should use the same permissions.
**FileXpress Gateway Administrator**

These Gateway Administrator data files are located in subdirectories in the FileXpress Gateway installation folder. The default location is:

C:\Program Files\Attachmate\FileXpress\Gateway\n
<table>
<thead>
<tr>
<th>Subdirectory</th>
<th>Data description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\GatewayAdministrator\conf\container.properties</td>
<td>Gateway Administrator properties file (page 88).</td>
</tr>
<tr>
<td>\GatewayAdministrator\services\directory\data\</td>
<td>FileXpress LDAP directory data. This directory contains user information, including hashed passwords.</td>
</tr>
<tr>
<td>\GatewayAdministrator\services\pemgmt\data\</td>
<td>FileXpress LDAP directory data.</td>
</tr>
<tr>
<td>GatewayAdministrator\services\directory\META-INF\replicadata.xml</td>
<td>Supports Gateway Administrator clusters.</td>
</tr>
<tr>
<td>\GatewayAdministrator\etc\</td>
<td>eventQueue.rnd - Queued PTA events. emailQueue.rnd - Queued email events.</td>
</tr>
</tbody>
</table>

If the server stops for any reason, queued actions resume after a server restart using information stored in these queue files. Deleting these files empties the queues.

*.cer and *.jks – Gateway Administrator certificates and keystore files

**Caution:** Do not delete any of the existing certificates or keystore files in these locations. The server certificates located here are required for communication between FileXpress Gateway components. Deleting the Gateway Administrator's server keystore and certificate will cause authentication of LDAP users to fail. If your Gateway Administrator Administrators group consists entirely of users in remote LDAP directories, you will no longer be able to log on to Gateway Administrator.

**FileXpress Transfer Server**

These Transfer Server data files are located in subdirectories in the FileXpress Gateway installation folder. The default location is:

C:\Program Files\Attachmate\FileXpress\Gateway\
Subdirectory | Data description
--- | ---
\TransferServer\conf\container.properties | Transfer Server settings
\TransferServer\etc\ | Transfer Server certificates

Caution: Do not delete any of the existing certificates or keystore files in these locations. The server certificates located here are required for communication between FileXpress Gateway components.

FileXpress Secure Shell Proxy

Directory | Data description
--- | ---
C:\ProgramData\Attachmate\RSecure Server\ | FileXpress Secure Shell Proxy settings, server certificates, key files, and the credential cache

Backing Up Gateway Administrator Data

To back up your current Gateway Administrator configuration, or move your configuration to a different system, copy the files listed below. These are installed to the following location by default:

C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\n
- \conf\*.*
- \etc\*.*
- \services\directory\META-INF\replicadata.xml
- \services\directory\data (include all subdirectories)
- \services\peermgmt\data (include all subdirectories)
- If you have installed a commercial certificate, back up the appropriate .jks, .p12, or .pfx file, as specified in the properties (page 88) file using the servletengine.ssl.keystore setting.
Managing the FileXpress Gateway Services

In this Chapter

- Start and Stop the FileXpress Gateway Administrator Service 94
- Start and Stop the FileXpress Transfer Server 94
- Start and Stop the FileXpress Secure Shell Proxy 95
- Change the Privileges of the Gateway Administrator Service 95
- Reset the Gateway Administrator to All Defaults 96
- Change the FileXpress User Access Account on the FileXpress Secure Shell Proxy 97

Start and Stop the FileXpress Gateway Administrator Service

The FileXpress Gateway Administrator service starts by default when you restart Windows. You can also use the Windows Services console to start and stop this service.

To start or stop the FileXpress Gateway Administrator service using the Windows Services Console

1. On the FileXpress Gateway Administrator computer, open the Windows Services console (Start > All Programs > Administrative Tools > Services).
2. Select the service called 'Attachmate FileXpress Gateway Administrator' and click start, stop, or restart.

Note: After the service has started, the FileXpress Gateway Administrator might not be immediately accessible. If you cannot connect to Gateway Administrator, wait a minute or two and try again.

Start and Stop the FileXpress Transfer Server

The FileXpress Transfer Server is the application server for the Transfer Client and also communicates with the FileXpress Gateway Administrator to authenticate FileXpress users. This server starts by default when you restart Windows. You can also use the Windows Services console to start and stop this service:

To start or stop the FileXpress Transfer Server service

1. On the FileXpress Proxy computer, open the Windows Services console (Start > All Programs > Administrative Tools > Services).
2 Select the service called "Attachmate FileXpress Transfer Server" and click start, stop, or restart.

---

**Start and Stop the FileXpress Secure Shell Proxy**

The FileXpress Secure Shell Proxy starts by default when you restart Windows. You can also use either of the following methods to start and stop this server.

**To use the FileXpress Secure Shell Proxy console**

1 Start the FileXpress Secure Shell Proxy console from the Start menu (or Apps list). It is installed under **Attachmate FileXpress Gateway > FileXpress Secure Shell Proxy**.

2 Use the **Action** menu items or the toolbar buttons to start and stop the server.

**To use the Windows Services console**

1 On the FileXpress Proxy computer, open the Windows Services console (**Start > All Programs > Administrative Tools > Services**).

2 Select the service called "Attachmate FileXpress Secure Shell Proxy" and click start, stop, or restart.

**Change the Privileges of the Gateway Administrator Service**

By default, the Gateway Administrator runs using the Network Service account, which has limited privileges. This helps ensure the security of your system by reducing the risk of an elevation of privilege attack, but might also prevent Post Transfer Actions from running in some configurations.

If you are running all three FileXpress Gateway services on the same system, and if you use the default **File Storage** setting (**FileXpress Gateway Proxy**), Post Transfer Actions run as a local process using the privileges of the Gateway Administrator service. The default privileges of this service are insufficient to execute most actions. To support running these actions, you can modify the Gateway Administrator service to use the privileges of the Local System account.

**To increase the privileges of the Gateway Administrator Service by running as the Local System account**

1. On the FileXpress Gateway Administrator computer, open the Windows Services console (**Start > All Programs > Administrative Tools > Services**).

3 Right-click the Attachmate FileXpress Gateway Administrator service, select **Properties**, then select the **Log On** tab.

4 Set **Log on as** to **Local System account** and click **OK**.

5 Click **Restart the service**.
To set the privileges of the Gateway Administrator Service to the default Network Service setting

2. From the Windows Services console, right-click the Attachmate FileXpress Gateway Administrator service, select Properties, then select the Log On tab.

6. Click This account, clear the Password and Confirm password fields, then click Browse.

7. Under Enter the object name to select, type in “network” and click Check Names. Your entry should be replaced by NETWORK SERVICE.

8. Click OK to close the open dialog boxes.

9. Click Restart the service.

Notes

- If you migrate from a configuration with all services on one system to a configuration that uses an SFTP server for file storage, you should reset the service to run using the Network Service account.

- The Gateway Administrator service reverts to the default profile after each upgrade.

Reset the Gateway Administrator to All Defaults

FileXpress Gateway Administrator installs a reset batch file that resets the Gateway Administrator to the original shipping state. Running this batch file has the following effects:

- Deletes all users and groups you have added to the FileXpress LDAP server and restores the default *admin* account.

- Deletes all transfer sites.

- Deletes all post transfer actions.

- Restores all system settings to the original defaults.

- Deletes any queued actions and emails.

Caution: Resetting the Gateway Administrator removes all saved users, transfer sites, and system settings. Use this option only to clear the data after initial testing, or if you cannot access the server with any available credentials and understand that all existing data and customizations will be lost.

To reset the Gateway Administrator to factory defaults

1. On the Gateway Administrator computer, open a command window using the "Run as administrator" option. (Start > All Programs > Accessories, right-click Command Prompt > Run as administrator.)
2 Navigate to GatewayAdministrator\bin in the FileXpress Gateway installation folder. The default location is:

`C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\bin`

3 Enter the following command:

`resetserver.bat`

You will see a prompt asking if you want to reset the Gateway Administrator to its initial state.

4 Press `Y`.

Without any further confirmation, the script stops the service, removes all saved user data and system settings, then restarts the service.

5 Wait a few minutes, then connect to the Gateway Administrator and log in using "admin" and "secret".

---

**Change the FileXpress User Access Account on the FileXpress Secure Shell Proxy**

The **FileXpress user access account** specifies the account on the FileXpress Secure Shell Proxy server that acts as the "run as" account for FileXpress users. FileXpress users run under the privileges provided by this account.

By default, **FileXpress user access account** is set to **Service account**. With this setting, FileXpress users run using the same account as the FileXpress Proxy Secure Shell Proxy service (the Local System account). Because of the privileges available to the Local system account, you should always leave **Restrict FileXpress users to file transfer sessions** enabled when **Service account** is selected. This is the default configuration.

To help further reduce the risk of escalation of privileges, you can use the following procedure to configure an alternate user account with more limited privileges than the Local System account.

*Note: The credentials for the account you configure must remain current or users will not be able to connect the FileXpress Transfer Server.*

---

**To change the FileXpress user access account**

1 Start the FileXpress Secure Shell Proxy console. It is installed in the Windows Start menu (or Apps list) under **Attachmate FileXpress Gateway > FileXpress Secure Shell Proxy**.

2 On the **FileXpress Users** pane, under **FileXpress user access account**, select **User account**.

3 Click **Select account**.

4 Click **Add** and enter the user name and password for the user whose account FileXpress users will run under. Click **Test** to confirm these credentials, then click **OK** to save this user account to the credential cache.

5 In the **Select Account** dialog box, select the user account you just added and click **OK** to set this as the "run as" account for FileXpress users.

6 Save your settings (**File > Save Settings**).
CHAPTER 12

Ensuring High Availability of the FileXpress Gateway Servers

In this Chapter

Create a Gateway Administrator Cluster 99
Configure Gateway Administrator for Failover and Load Balancing 102
Remove a Server from a Gateway Administrator Cluster 103
ConfigServer Command Line Utility 104
Configure Multiple FileXpress Proxy Servers 105

The procedures in this section describe how to configure a FileXpress Gateway environment to ensure high availability of file transfer services. The diagram below shows a sample configuration with two FileXpress Proxy Servers in the DMZ and two Gateway Administrators in the internal network.

- FileXpress Proxy server configuration is accomplished by manually copying configuration files between the server instances. No replication takes place between these servers. Once these servers are set up, changes are generally minimal and you can copy files manually as required after any settings change.

- The FileXpress Gateway configuration involves manually copying some configuration files and also setting up clustering, which provides ongoing replication of data between the servers. Changes you make to users and transfer sites from any Gateway Administrator in the cluster are automatically copied to all other members of the cluster.
Create a Gateway Administrator Cluster

The FileXpress Gateway Administrator server performs the following functions:

- Provides the web-based Gateway Administrator user interface for managing users and transfers.
- Authenticates users when they log on to the Transfer Client and communicates user and transfer site information to the FileXpress Proxy services.
- Stores user and transfer site information in the FileXpress database.

To maintain high availability of these services, you can configure a Gateway Administrator cluster. Data in the FileXpress database is automatically replicated across all servers in the cluster.

Setting up a cluster

To configure a cluster, you need to enable clustering on an initial Gateway Administrator server, copy required configuration files to each system you want to add to the cluster, then use the ConfigServer command line utility to add each member to the cluster. These procedures are detailed below.

There is no special master server in a cluster. Any existing cluster member can be used to add a new cluster member.

Before you begin

- Install FileXpress Gateway Administrator on the computers that will be part of your cluster. Every computer in the cluster must be resolvable in DNS. Members of a cluster communicate using DNS names. If DNS names are not resolvable, cluster members will not be able to provide data replication to other members of the cluster.
- If you use Post Transfer Actions, configure file storage on an SFTP server (page 74). If the FileXpress Gateway Proxy is used as the file storage server, and it is installed on the same system as one of the Gateway Administrator instances, actions will not run reliably.

Gateway Administrator cluster support is disabled by default in order to reduce the attack surface of the system. To enable cluster support, you need to edit the Gateway Administrator properties file (page 88) as follows.

To enable clustering in the Gateway Administrator properties file

1. Locate the container.properties file on the initial cluster server. The default location is:
   C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\conf

2. Set the following values and save the edited file.
   rmi.port.ssl = 43000
   replication.enabled= true
   directory.replication.port=8846

3. Restart the Gateway Administrator service (page 94).
Before you add a new Gateway Administrator server to a cluster, you need to copy some required configuration files to the new server. These files are not replicated automatically. If you have an existing Gateway Administrator that is already configured with users and transfer sites, use this as the initial cluster member.

### To copy required files to new members of the cluster

1. Locate the following files on the initial cluster server (or any server already added to the cluster) and copy them to each Gateway Administrator instance that you are adding to the cluster. This step is required because these files are not replicated.

   These files are installed to the following location by default:

   ```
   C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\Files\conf\*.*
   ```

   Notes:
   - Replace all files in the `conf` directory on the new instance with the files from the configured Gateway Administrator server. This directory includes the `container.properties` files, and other files that might contain customized logging settings.
   - `etc\servletcontainer.jks`
   - `Your commercial certificate in a .jks, .p12, or .pfx file`

2. Restart the Gateway Administrator service on the server to which you copied the files.

After you have enabled clustering and copied required files to a new server, you can use the ConfigServer utility to add the new server instance to the cluster. This initiates data replication between the added server and the cluster.

### To use the ConfigServer utility to add a server to the cluster

1. If there is a firewall between members of the cluster, open ports 43000 and 8846 on these computers.

2. If you have an initial FileXpress Gateway Administrator server that is already providing transfer services to users, back up your data for this server (page 93).

3. From any system with Gateway Administrator installed and clustering enabled, open a command window using the "Run as administrator" option (Start > All Programs > Accessories, right-click Command Prompt > Run as administrator).

4. Navigate to the FileXpress Gateway `bin` folder. For example:

   ```
   cd C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\bin
   ```
5 Run `configserver.bat` using the following syntax:

```bash
configserver -clusterserver <clusterserver> -clusteruser <admin> -clusterpassword <password> -instanceserver <instanceserver> -instanceuser <admin> -instancepassword <password> -command addserver
```

Replace the items in brackets with your values for each of the following arguments:

- **clusterserver**: The DNS name of a server that is already a member of the cluster. If you are creating a new cluster and you have a Gateway Administrator server that is already configured, use this server as the clusterserver.

- **clusteruser**: A user who can log on to Gateway Administrator running on clusterserver. This user must have **System setup** rights.

- **clusterpassword**: The password for clusteruser.

- **instanceserver**: The DNS name of the unconfigured Gateway Administrator server instance that you are adding to the cluster.

- **instanceuser**: A user who can log on to instanceserver. This must be a user with **System setup** rights. If you are adding a newly installed server, you can use the default "admin" account.

- **instancepassword**: The password for the user account in the new instance. If you used the default "admin" account in a new installation that you have not yet logged into, use "secret" as the password.

You should see a message similar to the following:

```
Server instanceserver.mydomain.com has been added to the cluster clusterserver
```

Depending on the FileXpress database size and the bandwidth between the servers, it might take between 30 seconds to 30 minutes for the added server to come back up. Once the added instance comes back up, it will have the same data as the other members of the cluster. Afterwards, any changes in any member of the cluster will be propagated immediately to the other members of the cluster.

**Data replication in a Gateway Administrator cluster**

After data is received by one member of a cluster, it starts replicating to all of the other servers in a cluster. This process starts about half a millisecond after the data is received. If there is a data conflict, then the last change is replicated throughout the cluster. For example, if a password for a user is changed on one Gateway Administrator and a different password is set for the same user on a different Gateway Administrator in the same cluster, then the latest password change will be replicated to all members of the cluster.

If a server instance in a cluster is down, then the data replication will occur both to and from that server as soon as it comes back up. If the network connection between server instances of a cluster goes down, a best practice is to restore the network connection prior to making configuration changes in any Gateway Administrator instance in order to minimize the risk of data conflicts.
Configure Gateway Administrator for Failover and Load Balancing

After you have created a cluster that includes multiple Gateway Administrative servers, you can use DNS to support failover and load balancing between the members of that cluster. Using DNS, you can create a symbolic host name that can be used to connect to any of the servers in your cluster. For example if you have created a cluster that includes fxgserver1, fxgserver2, and fxgserver3, you can set up a DNS entry with the alias GatewayAdministratorCluster, and add each of the servers in the cluster to that entry.

Once you have created the DNS alias, you will need to configure the FileXpress Secure Shell proxy to connect to the DNS alias (GatewayAdministratorCluster in this example). If one FileXpress Gateway server is not running, the proxy will connect to another server configured for the DNS entry, and failover support is achieved.

You can also use the DNS service to achieve load balancing support. Since data replication automatically occurs between all servers in the cluster, the FileXpress Secure Shell Proxy receives the same user and transfer site information regardless of which instance of the Gateway Administrator it is connected to.

Before you begin

- Create a Gateway Administrator cluster (page 99).

To create an alias (common name) to connect to any server in a cluster

- Recommended method: For ease of maintenance, configure your DNS server to set up failover support. The DNS server can return results in round-robin or random order for load distribution.

- Alternative method: If you do not have access to your DNS server, you can edit the hosts file (C:\Windows\System32\drivers\etc\hosts) on each FileXpress Proxy system:

For example:

```
# Hosts file on system "filexpressproxy01"
# First entry is the unique name for the local system
10.0.0.1 filexpressproxy01
# Common name for the FileXpress Gateway Administrator cluster
10.0.10.1 GatewayAdministratorCluster
10.0.10.2 GatewayAdministratorCluster
10.0.10.3 GatewayAdministratorCluster
```

The local unique system name is listed to avoid problems with reverse DNS lookups on some platforms. This is followed by lines for the cluster common name (one line for each system running the Gateway Administrator service).

For systems that have multiple network interfaces, all IP addresses should be listed.

Once you have created the alias, you need to configure the FileXpress Proxy to connect to this alias. The following procedure shows how to do this if you have a single FileXpress Proxy system. See Configure Multiple FileXpress Proxy Servers (page 105) if you have more than one.

To configure the FileXpress Proxy to connect to the alias host name


2. On the **Configuration** tab, click **FileXpress Users** in the left-hand panel.
Ensuring High Availability of the FileXpress Gateway Servers

3 Enable **Allow access to FileXpress users** if it is not already enabled.

4 Set **Gateway Administrator host** to the name of the cluster alias.

5 Save your settings (**File > Save Settings**).

6 Click **Activate and verify**. Click **Yes** when prompted to restart the FileXpress Transfer Server service.

After you have configured a DNS alias to point to a cluster of Gateway Administrator servers, you should only use the non-clustered name of a member of the cluster to access the Gateway Administrator web pages as described below. Web session information is stored in memory, and is not replicated across clusters, so if the web browser switches from one member of a cluster to another during a single browsing session, the session will fail.

If you use a load balancer in front of the Gateway Administrator cluster for scalability, then sticky sessions should be enabled on the load balancer so that a web browsing session stays on the same server.

**To access the Gateway Administrator web interface after configuring a DNS alias**

Use the host name of an individual cluster server. For example:

Cluster members: GatewayAdministrator01, GatewayAdministrator02

Cluster name: GatewayAdministratorCluster

In this example, you should access the cluster using one of the following URLs

https://GatewayAdministrator01:9490
https://GatewayAdministrator02:9490

Do not use https://GatewayAdministratorCluster:9490

**Remove a Server from a Gateway Administrator Cluster**

Use the **ConfigServer** command line utility to remove a server from a Gateway Administrator Cluster.

**Note:** Removing a server from a cluster restores the server to its initial state, with only the default "admin" account configured.

**To remove a server from a Gateway Administrator Cluster**

1 From any system with Gateway Administrator installed, open a command window using the "Run as administrator" option (**Start > All Programs > Accessories**, right-click **Command Prompt > Run as administrator**).

2 Navigate to the FileXpress Gateway bin folder. For example:

   cd C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\bin
Run `configserver.bat` using the following syntax, where the cluster server is the server that will remain in the cluster and the instance server is the server you want to remove from the cluster:

```
configserver -clusterserver <cluster server> -clusteruser <admin> -clusterpassword <password> -instanceserver <instance server> -instanceuser <admin> -instancepassword <password> -command removeserver
```

**ConfigServer Command Line Utility**

Use the ConfigServer command line utility to manage membership in a FileXpress Gateway Administrator cluster. It provides these services:

- Add servers to a FileXpress Gateway Administrator cluster
- Remove servers from a cluster
- List which servers are members of a cluster

The `configserver.bat` file is installed with FileXpress Gateway Administrator in the `bin` folder. The default location is:

```
C:\Program Files\FileXpress\Gateway\GatewayAdministrator\bin\configserver.bat
```

**Notes:**

- Before you use this utility, enable clustering in the Gateway Administrator properties file (page 88). For details, see Create a Gateway Administrator Cluster (page 99).
- To run this utility, open a Command Prompt using the Run as administrator option.

To view the usage help for this utility, run `configserver.bat` with no arguments, as shown here:

```
C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\bin>configserver.bat
```

**Sample ConfigServer Commands**

These examples show sample syntax and output of successful operations.

```
> configserver.bat -clusterserver nodoubt1 -clusteruser admin -clusterpassword secret -instanceserver nodoubt2 -instanceuser admin -instancepassword secret -command addserver

Server nodoubt2 has been added to the cluster nodoubt1

> configserver.bat -clusterserver nodoubt1 -clusteruser admin -clusterpassword secret -command listservers

Name,Address,ReplicaAddress,Online
nodoubt2,nodoubt2.acme.com:43000,nodoubt2.acme.com:8846,true
nodoubt1,nodoubt1.attachmate.com:43000,nodoubt1.attachmate.com:acme.com:8846,true

> configserver.bat -clusterserver nodoubt1 -clusteruser admin -clusterpassword secret -instanceserver nodoubt2 -instanceuser admin -instancepassword secret -command removeserver
```

104
Server nodoubt2 has been removed from the cluster nodoubt1

Configure Multiple FileXpress Proxy Servers

The FileXpress Gateway Proxy server runs two services:

- **FileXpress Transfer Server**
  Provides the Transfer Client web application. When users log in, the Transfer Server communicates with the Gateway Administrator web service to authenticate users.

- **FileXpress Secure Shell proxy**
  Creates transfer site directories on the designated file storage server and manages Secure Shell encrypted transfer between the user workstation and these directories. Communicates with the Gateway Administrator web service to get required information such as user authentication, transfer site access, and transfer site permissions.

To ensure high availability of these services, you can configure multiple FileXpress Proxy servers and use a DNS alias or third-party load balancer to distribute the load between these servers and provide failover support.

Note: By default, the FileXpress Gateway Administrator is configured to store files on the FileXpress proxy. This option is not supported if you use multiple FileXpress Proxy servers, because there is no replication of data between these servers. To support a configuration with multiple FileXpress Proxy servers, you must configure file storage on an SFTP server.

Setting up multiple FileXpress Proxy Servers

When you configure multiple FileXpress Proxy servers, each instance must be identically configured, and must be able to communicate securely with the Gateway Administrator web service. An internal password used to secure this connection is established when you click the **Activate and verify** button in the FileXpress Secure Shell Proxy. Each time you do this, the internal password is updated. This means that activating and verifying on one FileXpress Proxy in your group will invalidate the existing configuration of other FileXpress Proxies. To avoid this problem and to ensure your servers are identically configured, use the following procedures to set up one FileXpress Proxy server, then copy required files from this server to the additional servers.

**Before you begin**

- Install the FileXpress Gateway Proxy services on each computer you are configuring.

- Log onto the Gateway Administrator and go to **System > File Storage** and confirm that **SFTP server** is selected and that a connection to an SFTP server has been configured.

**To configure interchangeable FileXpress Proxy servers**

1. Select one FileXpress Proxy server for initial configuration. If you have an existing instance, use it. Start the FileXpress Secure Shell Proxy console on this server.

2. On the **Configuration** tab, click **FileXpress Users** in the left-hand panel.

3. Enable **Allow access to FileXpress users** if it is not already enabled.

4. Set **Gateway Administrator host** to the host name of your Gateway Administrator host or your cluster alias (page 102).
5  Save your settings (File > Save Settings).

6  Click **Activate and verify**. Click **Yes** when prompted to restart the FileXpress Transfer Server service.

   This action updates the Secure Shell Proxy’s `trustedWebService.cer` and `RSITDatabase` files; and the Transfer Server’s `trustedWebService.cer` and `container.properties` files.

7  On each destination server, stop the FileXpress Secure Shell Proxy (page 95) and the FileXpress Transfer Server (page 94).

8  Copy the required FileXpress Secure Shell Proxy configuration files (page 106) and FileXpress Transfer Server configuration files (page 107) to each destination server.

9  Restart the FileXpress services on each destination server.

   If you set up a DNS alias to provide load balancing and failover for your Proxy Servers, Transfer Client users will connect using this alias. If you use email notifications and are currently using a different server name, you need to update the base server URL used in email message links.

   **To update email notifications**

   1  Locate the properties file on the Gateway Administrator computer, and open it in a text editor. The default location of this file is:

   ```
   C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\conf\container.properties
   ```

   2  Edit the `transfer.server.url` setting to point to the DNS alias. For example:

   ```
   transfer.server.url=https://filexpresscluster.com:9492
   ```

   3  Save the edited properties file.

   4  Restart the Attachmate FileXpress Gateway Administrator service (page 94).

**Required FileXpress Secure Shell Proxy configuration files**

The following files used by the FileXpress Secure Shell Proxy must be manually copied to every FileXpress Proxy instance. Restart the FileXpress Secure Shell Proxy Server after making these changes. These files are located in the follow directory by default:

   ```
   C:\ProgramData\Attachmate\RSecureServer
   ```

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
</table>
| `rsshd_config.xml` | The FileXpress Secure Shell Proxy configuration file. The settings saved to this file include the values you have specified on the FileXpress Users tab for connecting to the Gateway Administrator host name and port.  
|                 | **Note:** If you modify any settings using the FileXpress Secure Shell Proxy, you need to redistribute this file to your duplicate servers. |
| `RSITDatabase`  | The FileXpress Secure Shell Proxy’s encrypted credential cache.               |
## Ensuring High Availability of the FileXpress Gateway Servers

### Required FileXpress Transfer Server configuration files

The following files used by the FileXpress Transfer Server must be manually copied to every FileXpress Proxy instance. Restart the Transfer Server after making these changes. These files are installed to the following folder by default:

```
C:\Program Files\Attachmate\FileXpress\Gateway\TransferServer\n```

**Note:** To simplify configuration, you can copy all files from the `conf` and `etc` folders. This list describes only the required files.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSITDatabase.sec</td>
<td>This file contains the key required to decrypt the credential cache and is required to use the cache.</td>
</tr>
<tr>
<td>trustedWebService.cer</td>
<td>Contains the public key used to authenticate FileXpress Gateway Administrator. This file is created when you click the Activate and Verify button on the FileXpress Users pane.</td>
</tr>
<tr>
<td>hostkey</td>
<td>The private key of the public/private host key pair used to authenticate this server.</td>
</tr>
<tr>
<td>hostkey.pub</td>
<td>The public key of the public/private host key pair used to authenticate this server.</td>
</tr>
<tr>
<td><strong>conf\container.properties</strong></td>
<td>The Transfer Server properties file. This file configures the Gateway Administrator host and port, and the internal password used for to secure the connection. If you have configured a certificate from a commercial CA, configuration information is also included in this file.</td>
</tr>
<tr>
<td><strong>etc\trustedWebService.cer</strong></td>
<td>The public key used for authenticating the Gateway Administrator.</td>
</tr>
<tr>
<td>etc\servletcontainer.jks</td>
<td>This is the default self-signed server certificate. If you are still testing and have not installed a certificate signed by a commercial Certificate Authority, copy this file to the other servers.</td>
</tr>
<tr>
<td><strong>-OR-</strong></td>
<td></td>
</tr>
<tr>
<td>Your CA-signed server certificate in a .jks, .p12, or .pfx file</td>
<td>If you have replaced the default self-signed server certificate with a certificate signed by a commercial Certificate Authority, copy the CA-signed certificate to the location specified in <code>container.properties</code> under <code>servletengine.ssl.keystore</code>.</td>
</tr>
</tbody>
</table>
Set Up File Transfer Auditing

You can use audit logging to maintain a record of file transfer activity. Audit logging is configured using the FileXpress Secure Shell Proxy. It is not enabled by default. The audit file is a comma-delimited text file with the following data for each transfer:

- User ID
- Client IP address
- Action (upload or download)
- Server filename
- Start time
- End time
- Server file modification time
- Server file size
- Bytes transferred
- Result (success or failure)
- Reason
- Server file hash (optional, the SHA-1 hash of the file contents)

**To enable file transfer auditing**

1. From the FileXpress Gateway Proxy, start the FileXpress Secure Shell Proxy console. It is installed in the Windows Start menu (or Apps list) under Attachmate FileXpress Gateway > FileXpress Secure Shell Proxy.
2. Go to Configuration > Logging > Audit Logging.
3. Select Enable file transfer auditing.
4. Save your settings (File > Save Settings).

When audit logging is enabled, FileXpress Secure Shell Proxy creates a new log each day in the specified Audit log directory. Audit logs use this name format: RSSHD-Audit-YYYYMMDD.log, where YYYYMMDD indicates the date.

To view the audit log quickly from the FileXpress Secure Shell Proxy console, use the audit log file toolbar button:
Change the JRE

The FileXpress Transfer Server and FileXpress Gateway Administrator are Java applications. A correctly configured Java Runtime Environment (JRE) is installed and used by default. Use the procedures below to configure these services to use a different JRE.

Notes:

- Each time you upgrade your JRE, you need to apply the unlimited strength policy files to the new JRE.
- Each time you upgrade FileXpress Gateway or apply a hotfix, you need to repeat the changes to the properties files.

Install a Java JDK from the Oracle site

2. Download and install the JRE using either the JDK download or the Server JRE download.
   - Download the latest Java 7 update. Java 8 is not supported.
   - The Server JRE is recommended. This download does not include the browser plug-in. Because this plug-in is where most of the security vulnerabilities are found, using this download helps reduce your security risk.

Note: Updates to JREs you download this way are not automatic, and each update uses a new, version-specific folder (for example C:\Program Files\Java\jdk1.7.0_<nn>\jre).

Apply the Unlimited Strength Jurisdiction Policy Files to your JRE

2. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.
3. Unzip the downloaded file and locate the following two policy files:
   local_policy.jar
   US_export_policy.jar
4. Locate the security folder in the Java install you want to use (<java-home>\jre\lib\security).
5 Replace the limited strength policy files in that folder with the unlimited strength policy files.

Note: You need to repeat this procedure each time you upgrade your JRE.

Edit the properties files and restart the servers

1 Locate the configuration properties file (container.conf) for both the Gateway Administrator and the Transfer Server:

<install path>\GatewayAdministrator\conf\container.conf
<install path>\TransferServer\conf\container.conf

2 Open each of these files in a text editor and locate the wrapper.java.command parameter. Edit this parameter to specify the full path to the java command (without the .exe extension) in your JRE. For example:

wrapper.java.command=C:\Program Files\Java\jdk1.7.0_<nn>\bin\java

3 Restart the Gateway Administrator Server (page 94) and the Transfer Server (page 94).

Note: You need to repeat this procedure each time you upgrade FileXpress Gateway or apply a hotfix.
CHAPTER 15

Customize the Look of the Transfer Client Web Pages

By default, the Transfer Client uses Attachmate FileXpress names and images. You can modify these web pages so that Transfer Client users see a page title and the images that identify your organization.

To customize the Transfer Client web pages

1. Create a folder called `custom` in the `webapps` folder:
   
   `<install path>\TransferServer\services\webxfer-ui\webapps\custom`

   Note: Making changes in this location ensures that your modifications remain in place after a server restart or application upgrade. Changes made in other locations, or to the existing files, are not guaranteed to remain in place.

2. Locate the `custom-example` directory in `webapps` and copy the contents of this folder into your `custom` folder.

3. Edit `title.html`, replacing the sample title "Custom File Transfer" with the page title you want displayed in the user's browser.

4. View the contents of `branding.css`. This file configures images and related colors. Edit the styles to suit your design, create appropriate images as defined in this file, and replace the sample images with your custom images.

5. Connect to the Transfer Client or refresh the browser display to view the changes.
Chapter 16

Troubleshooting

In this Chapter

- Log Files .................................................. 112
- Transfer Client Troubleshooting .................. 114
- Password Troubleshooting ........................ 118
- Gateway Administrator Login Page Troubleshooting 119
- Email Troubleshooting ................................. 119
- Post Transfer Action Troubleshooting .......... 120
- Server Certificate Troubleshooting .............. 122

Log Files

Gateway Administrator and Transfer Server Logs

Log files for the FileXpress Gateway Administrator and the FileXpress Transfer Server are created in the logs folders:

<install path>
\GatewayAdministrator\logs

<install path>
\TransferServer\logs

Note: By default, the server log files and debug log files (when debug logging is enabled) roll over daily and are deleted after three days. This helps ensure that disk space is not used up by large, accumulating log files. If you alter the configuration to keep these files for a longer period, you should monitor the files and/or move them to another server to ensure that sufficient disk space is always available.
The following log files are available for both FileXpress Gateway Administrator and the FileXpress Transfer Server:

**console.yyyymmdd.log**

This is the primary troubleshooting log. By default, console logs roll over daily and include the date in year-month-date format. These files are not deleted.

To modify console log rollover, logging levels, and log deletion, use container.conf.

**server.log**

**server.yyyymmdd.log**

This file rolls over daily. The file called server.log captures log information for the current day. By default, rolled-over log files include the date in year-month-date format, and logs are deleted after three days. Only the first 15 lines of an exception are shown.

**debug.log**

Debug logging is not enabled by default and is rarely needed. A debug.log file is created in the logs folder, but remains empty unless you enable debug logging.

To enable debug logging, edit logback.xml. The lines to edit and for instructions for making the change are under LOG SET-UP.

The following additional log is available for the Gateway Administrator:

**directory.log**

The directory log contains logging related to the built-in FileXpress LDAP directory transactions.

To modify the directory log settings, use logback.xml.

Additional instructions for customizing logging are included in the logback.xml and container.conf files. You need to restart the server after editing these files. These files are located in the conf folder:

```
<install path>\GatewayAdministrator\conf
<install path>\TransferServer\conf
```

Note: Edits you make to logback.xml and container.conf need to be repeated each time you apply a hotfix or upgrade FileXpress Gateway.
**FileXpress Secure Shell Proxy Logs**


**Windows Event Viewer**

Logging to the Event Viewer is enabled by default.

To view the Event Viewer log from the FileXpress Secure Shell Proxy console, click the toolbar button, or go to View > Event Viewer.

To modify the Event Viewer log level, go to Configuration > Logging > Event logging.

**Text file logs**

Logging to text files is not enabled by default.

To enable logging to a text file, set the log level, specify a log file directory, and configure rollover, go to Configuration > Logging > Debug logging.

To view the log file from the FileXpress Secure Shell Proxy console, click the toolbar button, or go to View > Latest Debug Log File.

---

**Transfer Client Troubleshooting**

**The Browser Cannot Display the Web Page**

**Problem:** The browser displays a message saying it is unable to display the Transfer Client log in page.

- Is the Transfer Server running?

  Open the Windows Services console (Start > All Programs > Administrative Tools > Services) and confirm that the Attachmate FileXpress Transfer Server is started.

  Note: It might take awhile after the service has started in the Windows Services console before you can log in. To confirm that all startup processes are complete, open the Transfer Server server.log file (page 112) and look for "Verastream Server Container started."

- Is the required port open in the firewall?

  Check that port 9492 is open inbound on the system running the FileXpress Transfer Server.

- Is the server certificate correctly configured?

  See Server Certificate Troubleshooting (page 122).

**Problem:** The browser displays the message, "HTTP ERROR 403 Problem accessing /webxfer/ui/. Reason: Forbidden"

- This message may appear if you launch an additional FileXpress Transfer Client in a browser session that already has run the Transfer Client. To resolve the issue, close all instances of your browser, then connect to the Transfer Client.
Password Login Fails at the Transfer Client Login Page

To troubleshoot Transfer Client login issues, use the Transfer Server console log. The default location is:

C:\Program Files\Attachmate\FileXpress\Gateway\TransferServer\logs\console.yyyymmdd.log

Also review the following troubleshooting guidelines.

Problem: The user sees an error message that says, "The username or password you entered is incorrect" or the login page refreshes without displaying any error.

- Has the user been added to the Gateway Administrator?
  In Gateway Administrator, click the Users tab and search each of the configured LDAP servers to confirm that the user exists.

- If the user exists, is the password correct?
  If a user in the FileXpress LDAP server has forgotten the password, you can edit the user in Gateway Administrator to change the password.

- If the user is in an added LDAP server, has the user entered the correct credentials for their user name on the LDAP server?
  Connect to Gateway Administrator, go to System > LDAP Servers, select your server, click Edit, and check the values configured for Domain Name and Advanced domain settings.

Problem: The user sees an error message that says, "Server not configured. Please contact your system administrator."

- Is FileXpress user access configured on the FileXpress Secure Shell Proxy?

- Have configuration changes affected the connection between the FileXpress Proxy and the Gateway Administrator?

Problem: The user sees an error message that says, "An unknown error has occurred. Please try again later or contact your system administrator."

- Are the services running and available?
  If you just restarted your Windows computer or just started your Gateway Administrator or the Transfer Server, wait a minute and try again. These services take a few moments to become available.

  To confirm that the services are running, on each system, open the Windows Services console (Start > All Programs > Administrative Tools > Services) and confirm that the Attachmate FileXpress services are all running.

- Are required ports open in your firewall?
  Check that port 9190 is open from the FileXpress Gateway Proxy to the FileXpress Gateway Administrator. See Ports and Firewall Configuration (page 13).
Have you made configuration changes that affect the connection between the FileXpress Proxy and the Gateway Administrator?


Is clustering correctly configured?

If Gateway Administrator servers are configured with different server certificates, users might see this error when they attempt to log in.

### Transfer Client Login Succeeds but the Server Connection Fails

The initial login to the Transfer Client succeeds and the Transfer Client user interface displays, but the user does not get a successful connection to the server.

**Problem:** The message "**Connection failed: <User name>**" appears in the menu bar next to the Logout button and no error message dialog box is displayed.

- Confirm that the FileXpress Secure Shell Proxy service is running. On the FileXpress Proxy server, open the Windows Services console (Start > All Programs > Administrative Tools > Services). Confirm that "Attachmate FileXpress Secure Shell Proxy" is started.
- If you are using a firewall, confirm that port 22 is open inbound to FileXpress Proxy server.

**Problem:** A dialog box appears with the error message "**User authentication failed. Exit Code 14**" or the "**Connecting**" message hangs and is not followed by a successful connection. To troubleshoot these problems, start the FileXpress Secure Shell Proxy console (Start > All Programs > Attachmate FileXpress Gateway > FileXpress Secure Shell Proxy).

- On the FileXpress Users pane, confirm that **Allow access to FileXpress users enabled**.
- On the FileXpress Users pane, click **Activate and verify**. The Web service connection dialog box will display a series of messages. If the connection is successful, the last message will read "Web service connection has been verified." If you see this message, the configuration changes made might have corrected the problem.
- If you configured a **User account**, confirm that the credentials are valid. On the FileXpress Users pane, click **Select account**. Select the account name, click **Edit**, then click **Test**.
- Are there permissions settings denying login access? Check the Permissions pane and the Access Control panes. You can also determine if permission is denied by looking for warning messages in the FileXpress Secure Shell Proxy server log file (page 112).

**Problem:** A dialog box appears with the error message "**Unable to Initialize.**"

- Are you connecting from a Windows server using Internet Explorer with enhanced security enabled?

Go to Start > Administrative Tools > Server Manager. In the Server Manager, click the top node (Server Manager) Under **Server Summary**, expand **Security Information**, and click **Configure IE ESC**.

Refer to the FileXpress Secure Shell Proxy log file (page 112) for additional information. To confirm that the client applet is working and able to connect to the server, look for "Connection from" followed by the client IP address. Check the timestamp and look for messages that follow the connection you are troubleshooting.
Server Connection Succeeds but the Transfer Fails

The user makes a successful connection to the Transfer Client but is unable to transfer files.

**Problem:** The user sees an error message that says, "**Failed to change to remote directory <directory name>**."  
- Confirm that your File storage server is running. This message appears if a user attempts to drill down into transfer site directories when the SFTP server is down.

**Problem:** The user sees an error message that says, "**Unable to execute the file transfer request. The remote directory <directory name> must exist.**"  
- Confirm that your File storage server is running. This message appears if a user attempts to upload a file when the SFTP storage server is down.

**Problem:** User has difficulty managing drag-and-drop functionality.

- As an alternative to drag-and-drop, right-click a local file and select **Send file**, or right-click a server file and select **Receive file**.

**Problem:** The user sees an error message that says, "**The transfer operation to the host has failed or was canceled. Would you like to delete the remote file?**"  
- This message indicates that a transfer is interrupted. Clicking Yes or No determines whether or not a partially uploaded file remains on the server.

Certificate Authentication Fails

**Problem:** After a user connects to the Transfer Client, the error message says, "**X.509 client authentication is required. Please ensure you are passing a valid X.509 certificate that corresponds to a valid user in the system.**" This message appears when Gateway Administrator is configured to require authentication using X.509 certificates and authentication is not successful. This may be due to any of the following:

- PKI Services Manager is not running or is not correctly configured in the Gateway Administrator.
  
  Try testing the connection to PKI Services Manager from Gateway Administrator. Go to **System > PKI Servers**. Select your added server, click **Edit**, then click **Verify Connection**.

- No certificate is available on the client system.
  
  Has the client system been configured to use a smart card or present a personal certificate from the browser’s personal certificate store?

- The certificate is mapped to an invalid user account or is mapped to multiple user accounts.
  
  The PKI Services Manager identity mapping must return a single, valid user for the presented certificate. Use the PKI Services Manager test utility to view allowed identities. (Start the PKI Services Manager console and go to **Utility > Test Certificate**.) The allowed identity list should consist of exactly one user, and that user must be provisioned in Gateway Administrator.

- The certificate is valid, but PKI Services Manager is not correctly configured to validate it.
  

- The certificate presented by the user is invalid.
The certificate is expired, has been revoked, or does not meet other certificate requirements for user authentication. Use the PKI Services Manager test utility to test the certificate. (Start the PKI Services Manager console and go to Utility > Test Certificate.) For detailed information about certificate validation requirements, see "Certificate Attribute Requirements Enforced by PKI Services Manager" in the PKI Services Manager User Guide, which is available from http://support.attachmate.com/manuals/pki.html.

Managing Text File Line Endings

File transfers between the FileXpress Transfer Client and the FileXpress Secure Shell Proxy Server are always binary. This means that the content of transferred files, including text file line endings, is not modified in any way during the transfer. If you are managing text file transfers from systems that use different line endings (for example Mac or UNIX files transferred to the Windows server), use a text-file conversion utility to modify line endings.

Text file line ending conversion is configurable for file transfers between the FileXpress Secure Shell Proxy (page 74) and a remote SFTP server. Configure this from the Remote SFTP Server Connection dialog box using the Options tab. By default, files with .txt, .htm, .html, .bat, and .cmd are transferred as text files. You can modify this list of text file types, and specify which line ending convention should be used on the remote server for transferred text files. (The default is to determine the correct line ending automatically. Automatic line conversion is available if you are connecting to other FileXpress Secure Shell Proxy servers; it will not work with OpenSSH servers.)

For transfers involving all three systems (the Transfer Client, the FileXpress Secure Shell Proxy, and a remote SFTP server) where text conversion is configured and working on the FileXpress Secure Shell Proxy:

- All files exposed by the FileXpress Secure Shell proxy for download will have Windows line endings.
- The FileXpress Secure Shell Proxy expects all uploaded files to have Windows line endings.

Password Troubleshooting

If email password reset is not working, review the following possible causes.

Note: Administrators with the Manage FileXpress users role can update user passwords from Gateway Administrator. From the Users tab, select the user, click Edit, then click to expand Change password.

Problem: After clicking Reset on the password reset page, the user sees a message that says, "Time sensitive instructions to create a new password have been sent to the email address we have on record for this account..." but the user does not receive an email

- Confirm that email support is correctly configured (page 17).
- Because the Gateway Administrator provides access to sensitive information, users who are members of any group with access to the Gateway Administrator cannot reset their password using the Transfer Client reset link. These users will not receive any email notification after clicking the link. Users with the Manage FileXpress users role can reset their password using Gateway Administrator. Gateway Administrator users who do not have this role should contact a member of the Administrators or Transfer Site Administrators group.
**Troubleshooting**

**Problem:** After clicking **Reset** on the password reset page, the user sees a message that says, "An unknown error has occurred. Please try again later or contact your system administrator."

- This indicates that the connection to the Transfer Service failed. The log might include the message "Authentication failed for user rsitmodule."

  To resolve this, open the FileXpress Secure Shell Proxy. On the **FileXpress Users** pane, click **Activate and Verify**.

**Gateway Administrator Login Page Troubleshooting**

**Problem:** The browser is unable to display the Gateway Administrator log in page.

- Is the Gateway Administrator service running?

  Open the Windows Services console (Start > All Programs > Administrative Tools > Services) and confirm that the Attachmate FileXpress Gateway Administrator is started.

  **Note:** It might take awhile after the service has started in the Windows Services console before you can log in. To confirm that all startup processes are complete, open the Gateway Administrator server.log file (page 112) and look for "Verastream Server Container started."

- Is the required port open in the firewall?

  Check that port 9490 is open inbound on the system running the Gateway Administrator.

- Is the server certificate correctly configured?

  See Server Certificate Troubleshooting (page 122).

**Problem:** There is no "Forgot password?" link on the Gateway Administrator login page.

- Email password reset is not available for Gateway Administrator users. This is by design to help ensure the security of Gateway Administrator data.

**Email Troubleshooting**

To troubleshoot email problems, use the Gateway Administrator console log file. The default location is:

C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\logs\console.yyyymmdd.log

Also review the following troubleshooting guidelines:

**Problem:** No email is being sent.

- To test the email server connection, go to **System > Email Server** and click **Test Connection**. If this test fails, confirm the **SMTP server** and **Port** values.

- After you confirm that the email server connection is working, try sending a test email. Go to **System > Email Templates** and click **Preview**. Enter your email address in the **To:** field and click **Send Test Email**. If this fails, see the next item.

**Problem:** The email server connection succeeds, but test email sent from the **Email Templates** page fails.
The sender name or address might be invalid. Open the Preview option and try replacing the token used for Sender address email with a valid email address for your server. If this fixes the problem, go to the Email Server page and replace the global Sender address on this page, or edit the template to use the valid address instead of the token.

Your server may require a valid user and password. If you omitted UserID and Password on the Email Server tab, enter valid credentials and test again.

Confirm that the Email Server settings for Secure connection meet the requirements of your email server.

**Problem:** The link in a FileXpress email leads to a web page not available error.

- Does the URL in the email point to "localhost" (https://localhost:9492/webxfer/ui/recovery.jsp)? This indicates that the base URL has not been updated from the default. Open the Gateway Administrator Properties File (page 88), edit the value of transfer.server.url, and restart the FileXpress Gateway Administrator service. For details, see Configure Email Support in FileXpress Gateway Administrator (page 17).

**Problem:** Email is generally working, but some specific email messages aren't sent.

- Confirm that the email address specified for the user is correct. An incorrectly entered email addresses will not result in an error in the console log. This error is handled by the SMTP server. Check for undeliverable mail notifications in the inbox of the user account specified in the Email Server tab.

- User registration email is sent only when a user is first added, not after subsequent edits. If the initial registration email fails because of an incorrect user address, correct the address on the Edit User page. You can manually update the password at this time. Or, users who know their user ID but have not yet set a password can create a password by clicking the link in a transfer site access email, and then using the Forgot password? option.

- Because the Gateway Administrator provides access to sensitive information, users who are members of any group with access to the Gateway Administrator cannot reset their password using the Transfer Client reset link. These users will not receive any email notification after clicking the link. Users with the Manage FileXpress users role can reset their password using Gateway Administrator. Gateway Administrator users who do not have this role should contact a member or the Administrators or Transfer Site Administrators group.

**Problem:** Email is not sent in a timely manner, is not sent at all, and/or the server starts showing very high CPU utilization

- You may have multiple queued email messages that are not being sent or are taking unexpectedly long to send. Check the event queue file (<install path>\GatewayAdministrator\etc\emailQueue.rnd). If this file is large (>500 KB), it suggests that failing emails are preventing other emails from being processed. To remove all queued emails, stop the Gateway Administrator service and delete this file.

---

**Post Transfer Action Troubleshooting**

**Gateway Administrator PTAs**

To view Gateway Administrator PTA output and error messages, use the Gateway Administrator console log file and look for entries that include TransferSiteEventHandler. The default location is:
Troubleshooting

C:\Program Files\Attachmate\FileXpress\Gateway\GatewayAdministrator\logs\console.ymmd.log

Also review the following troubleshooting guidelines:

- If the PTA doesn't run, confirm that the action is added to your transfer site.
- Check the log to see if any resolved arguments include spaces. Use double quotation marks around these tokens.
- If the log includes syntax errors, check to see if any resolved arguments include unsupported characters.
- If the log includes the error "Unable to complete Transfer Site action," check to see that the configured name and path specified for the PTA program are correct. If the the action configuration includes a full path to the executable program, confirm that the SFTP server user account has rights to access this path.
- If the log includes permission errors, check to see if the SFTP server user account has permissions to write to locations required by actions defined in the PTA. If you are using the default FileXpress proxy setting for file storage, review the configuration information in Configure PTAs in Gateway Administrator (page 39).
- If PTAs fail to execute and/or the server starts showing very high CPU utilization, you may have multiple queued PTA events that are not completing or are taking unexpectedly long to complete. Check the event queue file (<install path>\GatewayAdministrator\etc\eventQueue.rnd). If this file is large (>500 KB), it suggests that events that have not completed are preventing others from being processed. To remove all queued events, stop the Gateway Administrator service and delete this file.
- If you are running a Gateway Administrator cluster, confirm that you have configured file storage on an SFTP server (page 74). If the FileXpress Gateway Proxy is used as the file storage server, and it is installed on the same system as one of the Gateway Administrator instances, actions will not run reliably.

Reflection for Secure IT PTAs

To view Reflection for Secure IT PTA output and error messages, configure output to the debug (text) log file. For details, see Configure PTAs in Reflection for Secure IT.

Also review the following troubleshooting guidelines:

- Confirm that you saved your server settings after creating or modifying your action and that the action is enabled.
- If the PTA doesn't run, the expression for your filter might be incorrect. Try a test with the default filter (*.).
- Check the log to see if any resolved arguments include spaces. Use double quotation marks around these tokens.
- If the log includes syntax errors, check to see if any resolved arguments include unsupported characters.
Server Certificate Troubleshooting

Refer to these troubleshooting steps if you changed the server certificate used by the Transfer Server or Gateway Administrator server.

After any changes you make to server certificate setup, always perform both of the following before retesting:

1. Close all browser windows.
2. Restart the server whose certificate you are configuring. See Start and Stop the FileXpress Transfer Server (page 94) and Start and Stop the FileXpress Gateway Administrator Service (page 94).

Error messages shown below are from the console.yyyyMMdd.log (page 112) file.

Certificate warning still appears

- Did you close all browser windows and restart the server before retesting?
- Does the server name in the URL you are using match the server name(s) in the certificate?

Browser cannot display the web page

- Did you specify the correct password for servletengine.ssl.keystorepassword?

  In the log file, look for: "java.io.IOException: Keystore was tampered with, or password was incorrect"
Troubleshooting

- Is the keystore or PKCS#12 file in the location specified for servletengine.ssl.keystore?
  
  In the log file, look for: "java.io.FileNotFoundException: <path> (The system cannot find the file specified)"

- If you generated a JKS from a PKCS#12 file, did you use the same password?
  
  In the log file, look for: "java.security.UnrecoverableKeyException: Given final block not properly padded"

- Is your PKCS#12 file encrypted with a FIPS-approved algorithm? Note that OpenSSL and the Windows Certificate Manager do not currently encrypt the certificate using strong algorithms by default. PBE-SHA1-3DES is the only approved algorithm currently available. If you see the following log file error, either re-encrypt your file (page 86) or import it into a Java keystore (page 86).
  
  In the log file, look for: "java.io.IOException: Could not decrypt data"

Login is successful, but error messages appear in the log file

- The message "javax.net.ssl.SSLException: Fatal Alert received: Bad Certificate" appears repeatedly in the server and console log files.

  This exception is most likely to occur if the Transfer Server has not been updated to trust a new Gateway Administrator certificate. To resolve this issue, from the FileXpress Secure Shell Proxy console, go to the FileXpress Users pane and click Activate and verify.
Glossary of Terms

A

authentication

The process of reliably determining the identity of a communicating party. Identity can be proven by something you know (such as a password), something you have (such as a private key or token), or something intrinsic about you (such as a fingerprint).

C

CA (Certificate Authority)

A server, in a trusted organization, which issues digital certificates. The CA manages the issuance of new certificates and revokes certificates that are no longer valid for authentication. A CA may also delegate certificate issuance authority to one or more intermediate CAs creating a chain of trust. The highest level CA certificate is referred to as the trusted root.

D

digital certificate

An integral part of a PKI (Public Key Infrastructure). Digital certificates (also called X.509 certificates) are issued by a certificate authority (CA), which ensures the validity of the information in the certificate. Each certificate contains identifying information about the certificate owner, a copy of the certificate owner's public key (used for encrypting and decrypting messages and digital signatures), and a digital signature (generated by the CA based on the certificate contents). The digital signature is used by a recipient to verify that the certificate has not been tampered with and can be trusted.

E

encryption

Encryption is the process of scrambling data by use of a secret code or cipher so that it is unreadable except by authorized users. Encrypted data is far more secure than unencrypted data.

J

Java keystore

A Java keystore is used for storage and transportation of certificates and associated private keys. Use the Java keytool utility to manage keystore files.
PKCS

PKCS (Public Key Cryptography Standards) is a set of standards devised and published by RSA laboratories that enable compatibility among public key cryptography implementations. Different PKCS standards identify specifications for particular cryptographic uses. Configuring certificates for FileXpress Gateway you may work with the following PKCS file types.

PKCS#7 can be used to sign and/or encrypt messages. It can also be used to store certificates and to disseminate certificates (for instance as a response to a PKCS#10 message). Files in this format typically use a *.p7b extension.

PKCS#10 is used for certificate requests to a Certificate Authority (CA).

PKCS#12 is used for storage and transportation of certificates and associated private keys. Files in this format typically use a *.pfx or *.p12 extension.

X.509 certificate

See digital certificate (page 124).