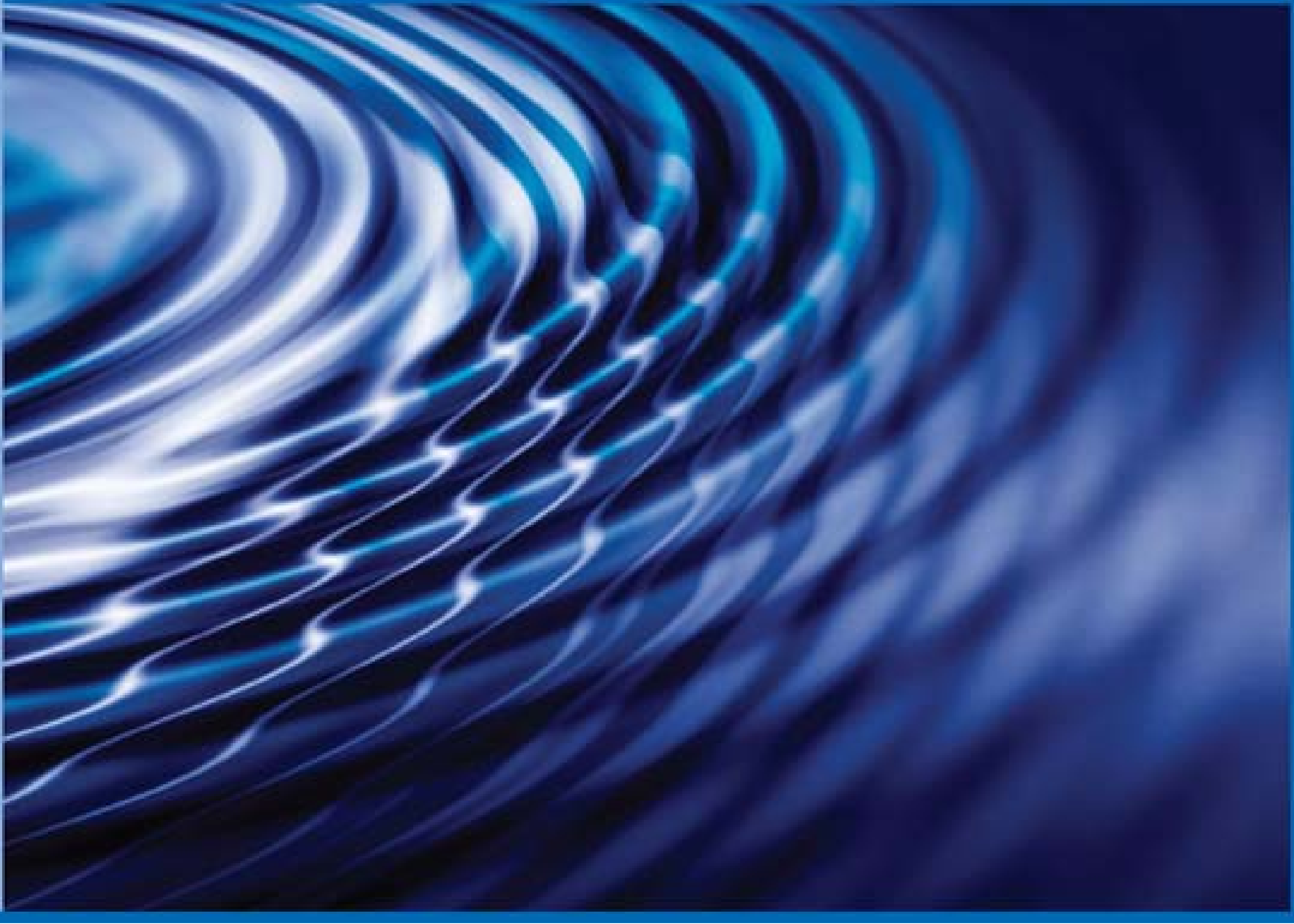
WEB EDITION
ADMINISTRATOR'S GUIDE

Attachmate® Reflection®

for Secure IT



RWE 8.1

Administrator's Guide

Reflection for Secure IT Web Edition

Version 8.1

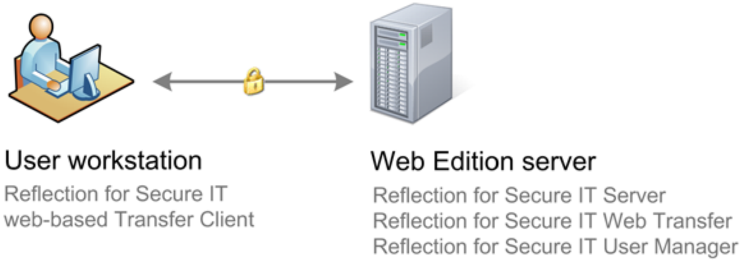
Attachmate

Contents

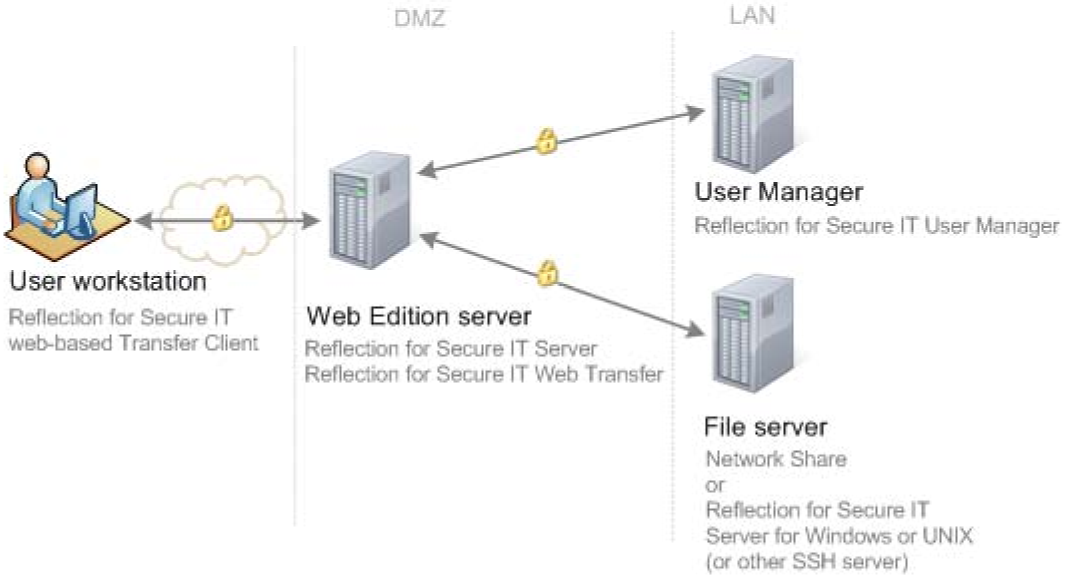
Introduction

Reflection for Secure IT Web Edition provides a secure way to manage file exchange with users outside your network. Secure authentication and encryption are used for all connections. Two possible configurations are shown below.

The simplest configuration has only two components. All Web Edition servers 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.


User workstation
Reflection for Secure IT
web-based Transfer Client
Web Edition server
Reflection for Secure IT Server
Reflection for Secure IT Web Transfer
Reflection for Secure IT User Manager

A typical distributed configuration is shown below. This configuration supports file exchange between users outside the network and a file server behind the firewall. It also puts the User Manager behind the firewall.


DMZ
LAN
User Manager
Reflection for Secure IT User Manager
User workstation
Reflection for Secure IT
web-based Transfer Client
Web Edition server
Reflection for Secure IT Server
Reflection for Secure IT Web Transfer
File server
Network Share
or
Reflection for Secure IT
Server for Windows or UNIX
(or other SSH server)

- User workstation

  Users log in to the web-based Reflection for Secure IT Transfer Client using a URL you provide. With this client, users can upload or download documents using an easy drag-and-drop interface.

- Web Edition server

  In both configurations, the Web Edition server runs the following two services

  - Reflection for Secure IT Web Transfer Server: Authenticates Web Edition users and is the application server for the Transfer Client.
  - Reflection for Secure IT Server for Windows: A Secure Shell server that manages secure file transfers.

  In the simplified configuration, you can also install the User Manager on this system.

  In the simplified configuration, files are uploaded and downloaded directly to and from this server. In the distributed configuration, the Web Edition server can be configured to act as a gateway to one or more file servers located behind your firewall. When you configure Web Edition to server as a gateway, data streams continuously through the gateway, eliminating the need to save the file on this server. This is more secure and more efficient than file transfer solutions that require the file to be stored and then forwarded.

- User Manager

  A web-based tool for configuring which users can log in to the Web Edition Transfer Client. You can use it to provide access to external users (such as customers or business partners) and to allow access to remote users (users with domain accounts working outside your firewall).

- File server

  You can configure one or more computers to act as the repository for uploaded and/or downloaded files. In the simplest configuration, you can upload and download files to and from your Web Edition server. However, in most cases you will use one or more additional file servers located behind your firewall. Users have access only to the directories you specify, and have no knowledge of the host name or the actual directory names on this server.

CHAPTER 1

Installation and Setup

In this Chapter

Web Edition Services

Reflection for Secure IT Web Edition installs three services. The installer includes all three services by default, and you can install all three services on one system for initial testing. In production environments, these services are typically divided between two different systems.

The following two services are always installed together. In a typical configuration you install these to a server located in the DMZ.

- Reflection for Secure IT Server

  A Secure Shell server that manages secure file transfers. You can use the server console to configure access to file locations on this server or on additional file servers. You can also configure customized file access for individual users or groups.

- Reflection for Secure IT Web Transfer

  Authenticates Web Edition users and is the application server for the Reflection for Secure IT Transfer Client. The Transfer Client is a Java applet that runs in the end user's web browser. This drag-and-drop transfer utility enables users to transfer documents between their local system and the file locations you have made available to them.

The User Manager is typically installed on a different system, located within your local area network.

- Reflection for Secure IT User Manager

  A web-based tool for configuring which users and groups have access.

Note: If you use smart cards, or other authentication systems that use X.509 certificates, you will also need to download and install Reflection PKI Services Manager. This add-on component is available free of charge with Reflection for Secure IT Web Edition. It is available on the Reflection for Secure IT Web Edition download page.

Web Edition Server Requirements

Reflection for Secure IT Web Edition is supported on the following platforms

- Windows Server 2012 (x64)
- Windows Server 2008 R2 (x64)
- Windows Server 2008 (x86, x64)
- VMWare vSphere Hypervisor (ESXi) running supported platforms

The User Manager is a web-based application. It has been tested on the following web browsers. JavaScript and cookies must be enabled.

- Microsoft Internet Explorer (version 8 or later, Windows only)
- Mozilla Firefox (version 12 or later)
- Google Chrome (version 26 or later)
- Apple Safari (version 6.0 or later, Mac only)

If your client users will authenticate using X.509 certificates, you need to install and configure Reflection PKI Services Manager, which is available at no additional charge from the Reflection for Secure IT Web Edition download page. If you are already running an earlier version of PKI Services Manager, you may need to upgrade your version to support Reflection for Secure IT Web Edition.

- Reflection PKI Services Manager version 1.2 SP2 or later

Note: For additional recommendations to help ensure a secure environment, see Security Recommendations for the Web Edition Server (page 65).

Transfer Client Requirements

Note: This guide describes how to manage transfers from user workstations using the Reflection for Secure IT Web Edition Transfer Client, but using this client is not a requirement. Web Edition users can also transfer files to and from the Reflection for Secure IT Web Edition server using any Reflection for Secure IT Secure Shell client or other Secure Shell (SSH) client.

The Reflection for Secure IT Web Edition Transfer Client is a Java applet that runs in a web browser. Client workstations must meet these requirements.

Users must be running one of the following supported browsers. JavaScript and cookies must be enabled.

- Microsoft Internet Explorer (version 8 or later, Windows only)

  Note: To connect to the Transfer Client using Internet Explorer running on Windows Server, disable Internet Explorer enhanced security (IE ESC) for administrators and users.

- Mozilla Firefox (version 12 or later)
- Google Chrome (version 26 or later)
- Apple Safari (version 6.0 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/

- By default, the Transfer Client requires Java version 7 Update 21 or later.

  Note: Apple systems running Mac OS X 10.6 and below come with Java pre-installed, and only support updates to Java version 6 (1.6.0_*nn*). To support users running on these systems, you need to modify the minimum required Java version, which is specified in the Web Transfer Server properties file (page 44). On systems running Mac OS X 10.7 (Lion) and above, Java is not pre-installed and users can get the latest Java 7 from the Oracle website.

Install Web Edition

Before you install Reflection for Secure IT Web Edition, review the configuration options described in the Introduction (page 5).

- For the simplest configuration, you can install all services on a single system.
- For a distributed configuration, you'll need to run the installer twice: once to configure the Web Edition server (running the Secure Shell Server and the Web Transfer Server), and again to install the User Manager on a system behind your firewall.

Note: If you configure a distributed system, install the same version (and build) on all systems.

To install Reflection for Secure IT Web Edition from the download site

1 Log in to Windows with an Administrator account.

2 Click the download link and run the download program. Select a location for the installer files and click **OK**.

The files are extracted to the specified location, and the Attachmate Setup program starts.

3 On the **Feature Selection** tab, select the features you want to install. All features are installed by default. To remove a feature, click the icon next to the feature name and select **Feature will be unavailable**.

System you are setting up	Features to install
All services on a single system	Install all features (the default).
Web Edition server	Install **Secure Shell Server and Web Transfer**
User Manager	Install **User Manager**.

4 (Optional) To personalize the installation, click the **User Information** tab and enter the name, organization, and Volume Purchase Agreement (VPA) number (if you have a VPA).

Note: VPA numbers are used by customer support to expedite service requests.

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

6 Click **Install Now**.

The installer will install required prerequisites and then continue automatically to install the features you selected.

7 After the installation is complete you'll be prompted to restart Windows.

Note: The restart is required to complete the installation of the Reflection for Secure IT Secure Shell server. A restart also starts all installed services.

To confirm that the installed services are running

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

2. Confirm that the services you installed are running. (The services are not started by the installer, but are started automatically when you restart Windows.)

   Installed with the **Secure Shell Server and Web Transfer** feature:

   - Attachmate Reflection for Secure IT Server
   - Attachmate Reflection for Secure IT Web Transfer

   Installed with the **User Manager** feature

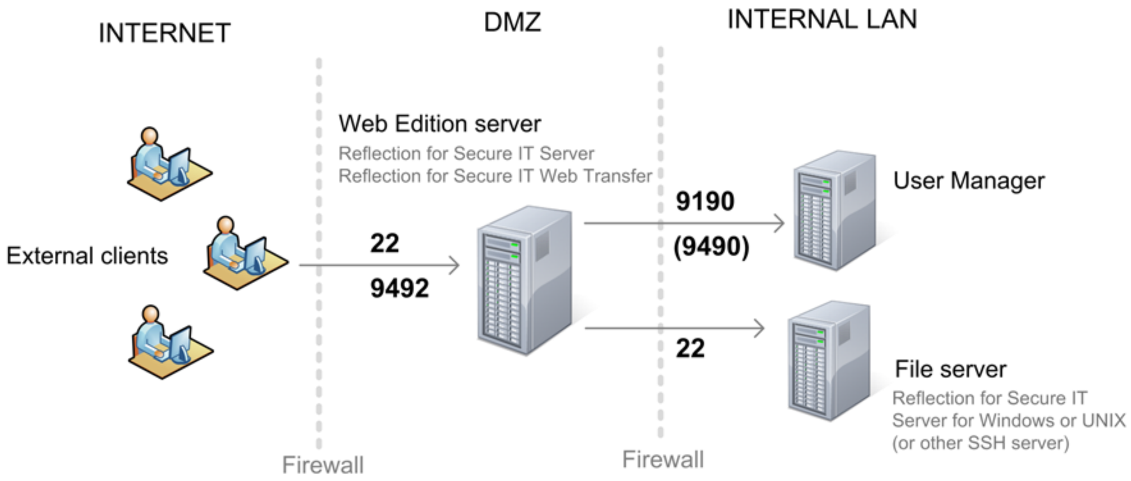
   - Attachmate Reflection for Secure IT User Manager

Note: After the Windows services have started, it may take several seconds before the web sites provided by these services are accessible.

Ports and Firewall Configuration

The following default ports are used in a distributed Reflection for Secure IT Web Edition configuration. The Web Edition server, which is typically installed in the DMZ, runs two services: the Reflection for Secure IT Server and the Reflection for Secure IT Web Transfer Server. These two services are always installed on the same system. The User Manager can be installed separately. Installing it behind a second firewall helps protect the user data stored on this system.

Port	Connection(s)
22	Secure Shell connections from external clients to the Reflection for Secure IT Server. Secure Shell connections to remote SFTP servers in your configuration.
9492	HTTPS connections from external clients to the Reflection for Secure IT Web Transfer Server.
9190	From the Web Edition server to User Manager.
9490	(optional) From the Web Edition server to User Manager. (Required if you want to launch User Manager from the Reflection for Secure IT Server console running in the DMZ.)



Upgrade from version 8.0

In Reflection for Secure IT Web Edition version 8.0, all three services were always installed on the same system. If you are upgrading from version 8.0, you can continue to run all services on the same system, or you can migrate to a distributed configuration (page 14).

To upgrade all services on one system

1 Log in as Administrator on your 8.0 server.

2 Install 8.1 over 8.0.

a) Install all features (the default).

b) Restart Windows after the 8.1 install is complete.

3 Move or copy any existing user files from the 8.0 folder structure to the 8.1 structure:

From: `<user profile>\ReflectionExternalUsers\Reflection.VirtualDirectory\`

To: `<user profile>\ReflectionWebEdition\Reflection\`

For example, if myuser is the name of your "run as" user, you could open a Command window and enter the following two commands :

```
mkdir C:\users\myuser\ReflectionWebEdition
```

```
move C:\users\myuser\ReflectionExternalUsers\Reflection.VirtualDirectory
C:\users\myuser\ReflectionWebEdition\Reflection
```

4 If you replaced the 8.0 Web Server self-signed certificate with a CA-signed certificate, or made any other changes to the Web Server `container.properties` file, you need to migrate your customizations as follows:

a) Move or copy your server certificates

From: `<install path>\WebServer\etc\`

To: `<install path>\WebTransfer\etc\`

b) Edit the version 8.1 properties file (`WebTransfer\conf\container.properties)` to include any modifications you made in the 8.0 file (`WebServer\conf\container.properties)`

5 Update the connection between the Reflection for Secure IT Server and the Web Transfer Server as follows:

a) Start the Reflection for Secure IT Server console. (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**.)

b) Click **Activate and verify**. (You'll be prompted to restart the Web Transfer Server; this restart will complete any changes you made to the container.properties file as well as completing the authentication update between the servers.)

Migrating to a distributed configuration

Use this procedure to continue to run the Reflection for Secure IT Server and the Web Transfer Server on your original system (typically in the DMZ) and install User Manager on a different system (typically one located in your internal network). See the Introduction (page 5) for a diagram of this configuration.

Upgrade Reflection for Secure IT Server and the Web Transfer Server on the 8.0 system

1 Log in as Administrator on your 8.0 server.

2 Run the 8.1 installer.

   a) On the **Feature Selection** tab, leave "Secure Shell Server and Web Transfer" selected.

   b) For "User Manager" choose "Feature will be unavailable."

   c) Restart Windows after the 8.1 install is complete.

3 Move or copy any existing user files from the 8.0 folder structure to the 8.1 structure:

   From: `<user profile>\ReflectionExternalUsers\Reflection.VirtualDirectory\`

   To: `<user profile>\ReflectionWebEdition\Reflection\`

   For example, if myuser is the name of your "run as" user, you could open a Command window and enter the following two commands :

```
mkdir C:\users\myuser\ReflectionWebEdition
```

```
move C:\users\myuser\ReflectionExternalUsers\Reflection.VirtualDirectory
C:\users\myuser\ReflectionWebEdition\Reflection
```

4 If you replaced the 8.0 Web Server self-signed certificate with a CA-signed certificate, or made any other changes to the Web Server `container.properties` file, you need to migrate your customizations as follows:

   a) Move or copy your server certificates

      From: `<install path>\WebServer\etc\`

      To: `<install path>\WebTransfer\etc\`

   b) Edit the version 8.1 properties file (`WebTransfer\conf\container.properties)` to include any modifications you made in the 8.0 file (`WebServer\conf\container.properties)`

Install the 8.1 User Manager on a different system

1 Log in as Administrator.

2 Run the 8.1 installer.

a) On the **Feature Selection** tab, leave "User Manager" selected.

b) For "Secure Shell Server and Web Transfer" choose "Feature will be unavailable."

c) Don't restart Windows after the 8.1 install. (If you already accepted the default to restart Windows after the install, stop the Reflection for Secure IT User Manager service.)

3 Copy the User Manager data files and folders from the following locations on the 8.0 system to the 8.1 system. (If you restarted Windows, there will be default content in these locations that was created when the service started. Overwrite this default content.)

```
<install path>\UserManager\services\directory\data\
```

```
<install path>\UserManager\services\peermgmt\data\
```

```
<install path>\UserManager\etc\
```

4 (Optional) If you used a CA-signed server certificate for User Manager on your prior system, you will need to replace the default server certificate (page 47) with a new certificate for your new host.

5 Start the Reflection for Secure IT User Manager service. (When you install only this service, a Windows restart is not required.)

Configure the Reflection for Secure IT Server to connect to the new User Manager host

1 Start the Reflection for Secure IT console (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**.)

2 Open the required User Manager ports (page 12) in your firewall.

3 On the **Web Edition Users** pane, change **User Manager host** to point to your new host.

4 Save your settings.

5 Click **Activate and verify**.

File Servers

You can configure one or more additional computers to act as the repository for uploaded and/or downloaded files. In the simplest configuration, you can upload and download files to and from your Web Edition server. However, in most cases you will use one or more additional file servers located behind your firewall. For a diagram showing a typical distributed configuration, see the Introduction (page 5).

Your file servers can be:

- Any servers available as network shares from the Reflection for Secure IT Server.
- Any system running a Secure Shell (SSH) server that includes an SFTP server.

For configuration details, see Configure Web Edition to Act as a Gateway (page 21).

CHAPTER 2

Getting Started

In this Chapter

In the procedures that follow, you'll create a sample user and perform test transfers using this user account.

Before you begin

- Install Reflection for Secure IT Web Edition and confirm that the services are running (page 10). For initial testing, you can install all services on one system, or set up a distributed configuration. See the Introduction (page 5) for diagrams of these options.

Launch User Manager and Add a Test User

In this procedure, you'll launch the Reflection for Secure IT Web Edition User Manager and add a test user.

To launch the User Manager

1 Start User Manager using either of the following methods:

If you are logged into the Windows system that is running User Manager, you can start User Manager from the Windows Start Menu (**Start** > **All Programs** > **Attachmate Reflection** > **Web Edition User Manager**).

-or-

From a web browser enter the following URL replacing *<user_manager_host>* with the name or IP address of the host running the User Manager service.

```
https://<user_manager_host>:9490
```

Note: The User Manager runs in your default browser and you will see a certificate warning message before you see the login page. This warning shows up because the User Manager 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 46).

2 For your initial login enter the following credentials.

Username: `admin`

Password: `secret`

3 Immediately after your first log in, you'll be prompted to change the password for the admin account. Enter the current and new password and click **Submit**.

Once you are successfully logged in, you should see the **Users** page. The initial view shows a single user - the admin account you used to log in.

To add a test user

1 From the **Users** page, click **New**.

2 On the **New User** page:

- Specify easy-to-remember values for UserID and password (or example test1/test1). You'll use these credentials for your test transfers.
- Enter sample values for first name, last name and email address; these are required fields.
- Leave group membership unchanged for this test user; group configuration is optional.

3 Click **Save**.

You'll be returned to the **Users** page and should see your new user added to the list.

Enable Web Edition User Access on the Reflection for Secure IT Server

To support file exchange using the Web Edition Transfer Client, you must configure the Reflection for Secure IT Server to allow access by Web Edition users.

Before you begin

- Select a Windows user account with rights to log on to the Web Edition server (the computer on which you installed the Secure Shell Server and Web Transfer feature). This account will act as the "run as" account for Web Edition users. Web Edition users will run using the privileges of this user account. You'll need to know the username and password for this account.

Note: To limit the access provided to Web Edition users, select a user account that is not a member of the Administrators group on this computer.

To enable access by Web Edition users

1. On the Web Edition server, start the Reflection for Secure IT Server console. (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**.)
2. On left panel of the **Configuration** tab, click **Web Edition Users**.
3. Enable **Allow access to Web Edition users**.
4. Leave **Restrict Web Edition users to file transfer sessions** enabled. This setting helps ensure the security of your server. Disabling it creates a risk that a knowledgeable Web Edition user might use a terminal session to gain access to directories that you have not made accessible to SFTP users. Leaving this setting enabled is particularly important if your Web Edition user account has administrative privileges.
5. For **User Manager host**, enter the name or IP address of the computer on which you installed the Reflection for Secure IT User Manager. If all Web Edition services are installed on the same computer, you can leave the default (localhost). Leave the default port value (9190). User Manager is configured by default to listen on this port.
6. Click **Select account**. Click **Add** and enter the user name and password for the user under whose account Web Edition users will run. Click **Test** to confirm these credentials, then click **OK** to save this user account to the credential cache.
7. 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 Web Edition users.
8. Save your settings (**File** > **Save Settings**).
9. Click **Activate and verify**. This triggers actions that ensure that the Reflection for Secure IT Server can establish a secure connection with the User Manager server. A dialog box display provides information about these steps. You will be prompted to accept the certificate presented by the User Manager server and to restart the Web Transfer service.
10. (Recommended) To help ensure security on this system, disable port forwarding for all users. On the left panel of the **Configuration** tab, click **Permissions**. Under **Tunneling**, clear the two port forwarding options.

Transfer Files to the Web Edition Server

The two test transfers described below save the transferred file to the Web Edition server.

Before you begin

- Enable Web Edition user access on the Reflection for Secure IT Server (page 18).
- Add a test user to the User Manager directory. (page 17) You'll need to know this user's UserID and password.

The first procedure transfers a document from one file location on the Web Edition server to another location on the same computer. This test scenario helps confirm that your setup is correct.

To test a transfer on the Web Edition server

1 On the Web Edition server (the computer on which you installed the Secure Shell Server and Web Transfer feature), start the Transfer Client. (**Start** > **All Programs** > **Attachmate Reflection** > **Web Edition Transfer Client**.)

> Note: The Transfer Client runs in your default browser and you will see a certificate warning message before you see the login page. This warning shows up because the Web 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 subsequent warnings. Before you deploy to actual users, you will need to install a certificate from a well-known Certificate Authority (CA). Once you've configured the Reflection for Secure IT Web Transfer server to use the CA-signed certificate, users will be able to log in without seeing certificate warnings. For more information, see Server Certificate Management (page 46).

2 Log in using the user ID and password of your test user.

You'll see two additional messages: a certificate warning followed by a Java query. Both messages include an option to trust content from this publisher, and, if you select this option, the messages won't appear again. (The certificate warning won't appear at all once you've configured the server to use a CA-signed certificate.)

3 The Transfer Client opens and connects to the running Reflection for Secure IT Server. Check to confirm that the status line in the lower left corner says "Connected to server."

4 On the left side of the client, under **Local files**, browse to locate a document for a test transfer and drag this file to **Server files**. After the transfer is complete, you should see the transferred file in the **Server files** list.

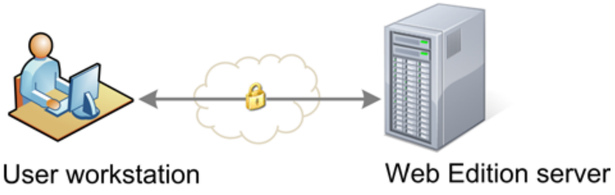
To locate the uploaded file on the Web Edition server

- Find the file you just transferred on the Web Edition server in the following location:

  `C:\Users\<run_as_user>\ReflectionWebEdition\Reflection\<web_edition_user>`

  Where *<run_as_user>* is the user account you selected for Web Edition users to run under and *<web_edition_user>* is the userID of the test user you created in User Manager.

The next transfer tests your ability to connect to the Transfer Client from a second computer and transfer a file from that computer to the Web Edition server. This test scenario confirms that your setup supports transfers from an external user's workstation.



To test a transfer from a second computer to the Web Edition server

1. To test a transfer from a user workstation, open a browser on a second computer.
2. Enter the following URL, replacing *<web_edition_host>* with the name or IP address of your Web Edition server. (This URL connects to the running Web Transfer Server).

   ```
   https://<web_edition_host>:9492
   ```

3. Log in using the test user credentials and try a test transfer.

Configure Web Edition to Act as a Gateway

In this procedure, you'll configure the Web Edition server (the computer on which you installed the Secure Shell Server and Web Transfer feature) to act as a gateway. This enables transfers to go between the user workstation and a back end file server. Two procedures are given below.

- Use the first procedure if the file server is available as a network share from the system running the Reflection for Secure IT Server.
- Use the second procedure if the file server is an SFTP server. This might be a Windows system running Reflection for Secure IT Server for Window or a UNIX system running Reflection for Secure IT Server for UNIX.

Configure the Reflection for Secure IT Server to connect to a network share

1. On the Web Edition server, start the Reflection for Secure IT Server console. (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**.)
2. From the **Configuration** tab, click **SFTP Directories** in the left panel, then click **Add**.
3. Enter a **Virtual directory** name (for example `Test)`. This is the directory name that users will see when they run the Transfer Client.
4. For **Local or UNC directory**, enter a UNC path that includes a server name and share. For example:

   ```
   \\server\share\public
   ```

5. Click **OK**.
6. In the **SFTP Directories** pane:
   - Set the **User login directory** to the virtual directory you just created, for example `/Test`. You'll see a warning message about changing the user key directory. Because Web Edition users do not use public key authentication, this is not a concern and you can click **Yes** to proceed.
   - Disable the default `Home` directory by clearing the Allow checkbox.
7. Save your settings (**File** > **Save Settings**).

Configure the Reflection for Secure IT Server to connect to an SFTP server

Before you begin

- Confirm that a Secure Shell server is installed and running on the host that will serve as your file server, and that SFTP is enabled. (SFTP is enabled by default on Reflection for Secure IT servers.)
- Confirm the DNS name or IP address for this host and know the port being used for Secure Shell connections (22 is the default).
- Confirm the name and password of a valid account on this host. This user account will provide access to file system on the file server.

To configure the connection to an SFTP server

1. On the Web Edition server, start the Reflection for Secure IT Server console. (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**.)
2. From the **Configuration** tab, click **SFTP Directories** in the left panel, then click **Add**.
3. Enter a **Virtual directory** name (for example `Test)`. This is the directory name that users will see when they run the Transfer Client.
4. Select **Remote SFTP server**. This opens the **Remote SFTP Server Connection** dialog box.

   Note: The "Remote SFTP server" you configure here is your back end file server.

5. For **Host**, specify the name or IP address of the file server. The port for the connection to this server is set to 22 by default. Edit this if your Secure Shell server uses a different port.
6. Under **Host key**, click **Retrieve**. Reflection for Secure IT connects to the Secure Shell server running on the file server, retrieves the host public key and displays a confirmation box. Click **OK** to accept this key and then close the **Get Public Key** dialog box.

   This key is used to confirm the host identity in subsequent connections, ensuring that documents are transferred to the correct host.

7. Under **Authentication**, for **Remote SFTP username** and **Password**, enter the credentials of the user account that will provide access to the file system on the file server.
8. Under **Remote base directory**, click **Browse**. This opens a browse dialog box showing directories available to the user you specified. (The directories available depend on this user's privileges and on how the SFTP server is configured.) Browse to select the directory you want to make available to your Web Edition users and click **OK**. The directory you select is entered in the **Path** field.
9. Click **Test Connection**. You should see a message saying that the connection was successful.

   Note: The **Test Connection** dialog box includes a Details button. You can use the information provided to troubleshoot this connection.

10 Close the dialog boxes and return to the **SFTP Directories** pane.

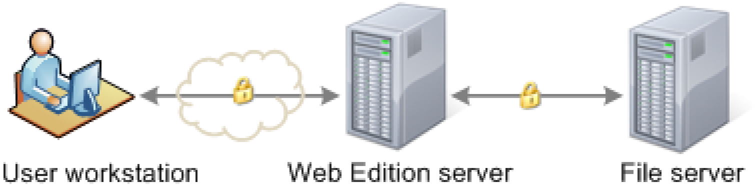
11 In the **SFTP Directories** pane:

- Set the **User login directory** to the virtual directory you just created, for example `/Test`. You'll see a warning message about changing the user key directory. Because Web Edition users do not use public key authentication, this is not a concern and you can click **Yes** to proceed.
- Disable the default `Home` directory by clearing checkbox in the **Allow** column.

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

Transfer Files to the Back End File Server

In this transfer, the document goes from the user workstation to your back end file server.



Before you begin

- Add a test user to the User Manager directory. (page 17) You'll need to know this user's UserID and password.
- Configure the Web Edition server to act as a gateway. (page 21)

To test a transfer from the user workstation to the file server

1 Open a browser on the computer you designated to act as a user workstation.

2 Enter the following URL, replacing *<web_edition_host>* with the name or IP address of your Web Edition server. (If you are already logged into the Transfer Client from a previous test, you can click Logout, and then log in again to test changes you've made on the Web Edition server.)

```
https://<web_edition_host>:9492/
```

Note: The Transfer Client runs in your default browser and you will see a certificate warning message before you see the login page. This warning shows up because the Web 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 subsequent warnings. Before you deploy to actual users, you will need to install a certificate from a well-known Certificate Authority (CA). Once you've configured the Reflection for Secure IT Web Transfer server to use the CA-signed certificate, users will be able to log in without seeing certificate warnings. For more information, see Server Certificate Management (page 46).

3 Log in using the username and password or your test user.

4 On the server side, you should see the files in the `Test` directory. (This is the **Remote base directory** you configured using the **Remote SFTP Server Connection** dialog box. The contents of this directory are displayed when the user connects because you set it as the **User Log in directory** in the **SFTP Directories** pane.)

5 Test an upload to the server from the client computer.

Confirm that your test file is on the server.

- If you uploaded to a network share, confirm that the file is in the location you specified in the **Accessible Directory Settings** dialog box for **Local or UNC directory**.
- If you uploaded to an SFTP server, log in to the SFTP server using the credentials you specified in the **Remote SFTP Server Connection** dialog box for **Remote SFTP username** and **Password**. Confirm that the file is in the location you specified under **Remote base directory**.

Set Transfer Permissions for a User Group

You can create customized transfer settings for individual users and for user groups. In this procedure you'll modify your Reflection for Secure IT Server settings to allow additional file access to members of the default "Administrators" group.

Note: The Administrators group used here is the only default group in the User Manager, and the default admin user is a member of this group. This procedure uses this default group for testing. Once you finish testing, you'll want to configure group access using your own groups. These can be groups you create in User Manager, or groups in any LDAP directory you add to User Manager.

Before you begin

- Configure (page 21) and test (page 23) a transfer to a back end file server.

Create a subconfiguration for members of the User Manager Administrators group

1 On the Web Edition server, start the Reflection for Secure IT Server console. (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**.)

2 On the left panel, under **Subconfiguration**, click **Group Configuration**.

3 Click **Add**. This opens the **Group Configuration** dialog box.

4 Set **Group type** to **Domain**.

5 For **Domain**, enter `Reflection`.

Use Reflection as the domain name for users or groups in the built-in User Manager directory. After you add additional LDAP directories to User Manager, you can also specify those domain names here.

Note: If you use groups from an added LDAP server, confirm that the domain name you specify here exactly matches the domain name specified in User Manager. (In User Manager, go to **LDAP Server**, select your server, click **Edit** and check the value entered for **Domain Name**.)

6 For **Group**, enter `Administrators`.

7 In the left portion of the **Group Configuration** dialog box, click **SFTP Directories**.

8 Click **Add**. This opens the **Accessible Directory Settings** dialog box. You'll use it to add access to a new folder that will be accessible to members of the Administrators group.

- For **Virtual Directory**, enter `AdminTest`.
- Click **Browse** and select any available local folder. It will be entered into **Local or UNC directory**. (For example `C:\Samples`.)
- Click **OK** to close the **Accessible Directory Settings** dialog box and return to the group configuration **SFTP Directories** page.

9 Use the drop-down list under **User login directory** to select **/**. (You added a second accessible directory and this change means that users in this subconfiguration will see all available directories when they log in.)

You'll see a warning about changing the user key directory. Because you are using password authentication for users, the warning doesn't apply to this test and you can click **Yes** to proceed.

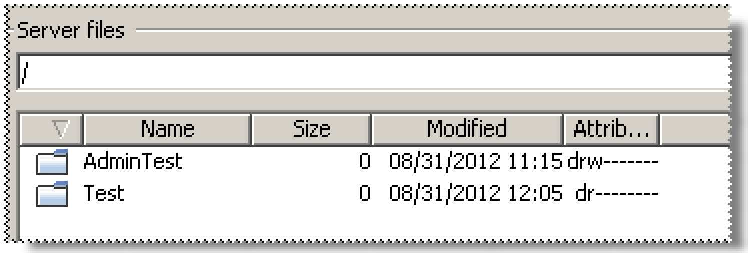
10 Click **OK** to close the **Group Configuration** dialog box.

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

Connect to the Transfer Client as a member of the Administrators group

1 From the user workstation, log on to the Transfer Client using the default admin account.

2 The Server file list shows two directories. In the image below, the first directory (`AdminTest`) is the directory on the Web Edition server that is available only to members of the Administrators group. The second directory (`Test`) is the directory on the back end file server that is available to all users.



Server files

/

Name	Size	Modified	Attrib...
AdminTest	0	08/31/2012 11:15	drw-------
Test	0	08/31/2012 12:05	dr--------

Note: If you've followed the procedures in this guide, these directories are on two different servers. `AdminTest` is on the Web Edition server. `Test` is on the back end file server. These actual server locations are not apparent to the Web Edition user.

3 Log out of the Transfer Client and log in again using your test user credentials to confirm that this user logs directly into the `Test` directory. You can browse up to the parent directory and confirm that this user has no view of the `AdminTest` directory.

CHAPTER 3

User Manager Administration

In this Chapter

Used alone, the Reflection for Secure IT Secure Shell server supports secure file transfer for internal users working within your network. These users have Windows domain accounts or local accounts on the server computer.

Reflection for Secure IT Web Edition User Manager enables you to provision additional users who need to upload or download documents securely. You can configure access for external users (for example, customers and business partners) and for remote employees of your organization (users who have accounts in your Windows Active directory, but are working outside your firewall).

Connect to the User Manager

The Reflection for Secure IT Web Edition User Manager is a web-based application. From the computer that is running the User Manager service, you can connect to User Manager from the Windows Start menu. From any system with network access to the User Manager, you can connect using a web browser.

To connect from the Windows Start menu

- On the computer running the Reflection for Secure IT User Manager service, go to **Start** > **All Programs** > **Attachmate Reflection** > **Web Edition User Manager**.

To connect from a web browser

- Enter the following URL, replacing *<user_manager_host>* with the DNS name or IP address of the host running the User Manager service.

```
https://<user_manager_host>:9490
```

Initial Login

User Manager is configured with a default administrator account and password. You need to change the password the first time you log in.

Note: The User Manager runs in your default browser and you will see a certificate warning message before you see the login page. This warning shows up because the User Manager 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 46).

To log in the first time

1 Connect to User Manager.

2 For your initial login enter the following credentials.

Username: `admin`

Password: `secret`

3 Immediately after you first log in, you'll be prompted to change the password for the admin account. Enter the current and new password and click **Submit**.

Add Users to the Reflection Directory

You can add users to User Manager's built-in Reflection directory when you want to exchange files securely with users who do not have accounts in your Windows Active Directory.

To add users to the User Manager Reflection directory

1 Connect to User Manager and log in as an administrator.

2 On the **Users** tab, click **New**.

3 Enter user information.

- Specify a password manually or click **Generate Password** to have User Manager automatically generate a password.
- (optional) Select **Require password change** to require users to change their password the first time they log in.
- Enter values in the required name and email fields.
- (optional) Specify group membership. Note that Group membership is not required and can be modified later.

4 Click **Save**.

Note: Before these users can transfer files, Web Edition user access must be enabled on the Reflection for Secure IT Server (page 18).

Add Users from Windows Active Directory

Use the **LDAP Servers** tab to provision users who have accounts in Windows Active Directory. You can use this approach to provide 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 provision users from an LDAP server

1 Connect to User Manager and log in as an administrator.

2 Click **LDAP Server**.

3 Click **New**.

4 Enter information for connecting to the server. For details, see LDAP Server Configuration (page 30).

5 Click **Test Connection** to confirm that User Manager can access your LDAP server.

Note: The Test Connection button verifies the connection but *does not save* your settings.

6 Click **Save**.

To view LDAP users and groups

Note: You can view users and groups that are brought in from an LDAP server, but cannot modify them; these users and groups are managed on the LDAP server.

1 Click the **Users** or **Groups** tab.

2 Use the drop-down list to select your LDAP server. If you don't see your server, return to the LDAP configuration page and confirm that you saved your settings.

LDAP Server Configuration

To add users from Windows Active Directory to User Manager, you need configure a new LDAP Server connection. The **New LDAP Server** includes the following settings for connecting to the server.

Type

Active Directory

This is not configurable; Windows Active Directory is the only LDAP directory supported in version 8.1.

Domain Name

The authentication domain name. This must be the name of the domain to which users authenticate. In the login `mydomain\myusername`, the authentication domain name is `mydomain`.

If users include a domain name when they log in, it must match the Domain Name you specify here.

Users can also log in without including the domain name. User Manager will search the domains for a match of the UserID and password provided. 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.

Server

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`)

Port

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 a global catalog port is recommended for better performance. For connections without using global catalog, the following ports are standard:

389 is standard for non-secure connections.

636 is standard for secure connections.

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 User Manager 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))`
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.

Configure Certificate Authentication

By default, users log in to the Transfer Client with a username 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 69).

  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, User Manager 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 listening port (18081 is the default).

- Client workstations must be configured to present certificates for user authentication. These can be done using CAC cards or by adding certificates to the browser's personal certificate store.

Configure User Manager to contact your PKI Services Manager

1. Connect to User Manager and log in as an administrator.
2. On the **Configuration** 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 69).
5. Click **Retrieve Public Key**.

   If the server is running and available, User Manager 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 **Verify Connection**. If User Manager 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 User Manager **Configuration** 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 username and password prompt. If a user certificate is available on the client system, User Manager 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.

Start and Stop the User Manager Server

The User Manager 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 Reflection for Secure IT User Manager service

1. Log on to the system running User Manager.
2. Open the Windows Services console (**Start** > **All Programs** > **Administrative Tools** > **Services**).
3. Select the service called "Attachmate Reflection for Secure IT User Manager" and click start, stop, or restart.

Note: After the service has started, it may take several seconds before the User Manager is accessible.

User Manager Properties File

You can use the User Manager properties file to modify the configurable settings listed below. It is located in the Web Edition installation folder in the `UserManager\conf` subfolder. The default location is:

```
C:\Program Files\Attachmate\RSecureWebEdition\UserManager\conf\container.
properties
```

Notes:

- You must restart the server (page 32) 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 User Manager. The default is 9490.

configservice-ws.port

The port used by the Reflection for Secure IT Server and the Web Transfer Server to communicate with the User Manager. This value must match the value configured in the Web Edition Users pane of the Reflection for Secure IT Server console and the Web Transfer Server properties file. (Clicking Activate and verify in the Web Edition Users pane automatically updates the value in the Web 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 47). The path must be specified using forward slashes or escaped backslashes. For example:

```
C:/pathto/keystore
```

```
C:\\pathto\\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.

Reset the User Manager Server to All Defaults

The User Manager installs a reset batch file that you can use to reset the User Manager and all user data to the original shipping state. Running this batch file has the following effects:

- Restores the original "admin" user with the default password "secret."
- Deletes all user data

Caution: Resetting the User Manager removes all user data. Use this option only to clear the data after testing or if you cannot access the server with any available credentials and understand that existing data will be lost.

To reset the User Manager and user database to the original state

1 On the system running User Manager, open a command window as a Windows administrator. (**Start** > **Accessories**, right-click **Command Prompt** > **Run as administrator**.)

2 Navigate to `UserManager\bin` in the Web Edition installation folder. The default location is:

```
C:\Program Files\Attachmate\RSecureWebEdition\UserManager\bin
```

3 Enter the following command:

```
resetserver.bat
```

You'll see a prompt asking if you want to reset the User Manager to its initial state.

4 Press `Y`.

5 The script stops the service, removes user data, then restarts the service.

6 Wait a few minutes, then connect to the User Manager and log in using "admin" and "secret". You'll be prompted to change your password.

CHAPTER 4

Reflection for Secure IT Server Configuration

In this Chapter

This guide describes Reflection for Secure IT settings that are relevant to Web Edition administrators. For additional information about administering the Reflection for Secure IT Server, refer to the help topics available from the server console.

Transfer Client File Locations

The Transfer Client shows a **Local files** list on the left and a **Server files** list on the right.

Local files

The Transfer Client's **Local files** list shows the contents of the user's profile folder. The user can browse from this location to any other folders and drives available to this user.

The user profile folder is configurable by the Windows system administrator. The default is:

- Windows 7, Windows Server 2008:
  `\Users\`*`username`*`\`

- Windows Server 2003:
  `\Documents and Settings\`*`username`*`\`

Server files

If you made no modifications to the default SFTP directories settings in Reflection for Secure IT, the **Server files** list shows the contents of a directory called "Home." This virtual directory corresponds to the following physical directory on the Web Edition server:

```
C:\Users\<run_as_user>\ReflectionWebEdition\Reflection\<web_edition_user>
```

where *<run_as_user>* is the **Web Edition user access account** (specified on the **Web Edition Users** pane in the Reflection for Secure IT Server), and *<web_edition_user>* is the user's **UserID** (added in the User Manager). When a user connects, this directory is created automatically if it does not yet exist.

If you provisioned users in an LDAP server, the domain name you specified for that server replaces "Reflection" in the path shown above.

Configure Access to Files on the Web Edition Server

If you made no modifications to the default SFTP directories settings in the Reflection for Secure IT Server, the **Server files** list shows the contents of the default Home (page 35) directory. You can use Reflection for Secure IT to customize the list of directories that users see. These can be local directories, directories on remote servers, or a combination of both. You can configure directory access to all users, or create subconfigurations (page 39) to customize access for particular users or groups.

Notes:

- The directories available to Web Edition users are limited by the rights of the user you specify for **Web Edition user access account** when you configure the Reflection for Secure IT Server.
- Transfer Client users have access only to directories that you explicitly make available. They do not have access to other directories, even if these directories are available to the **Web Edition user access account**.

To configure access to local directories

1. On the Web Edition server, start the Reflection for Secure IT console (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**).
2. From the **Configuration** tab, click **SFTP Directories** in the left panel.
3. Click **Add** and configure the directory settings in the **Accessible Directories Settings** dialog box.
   - For **Virtual directory**, specify the directory name you want users to see in the Transfer Client's **Server files** list.
   - For **Local or UNC directory**, specify the actual physical location of this directory. (Variables are supported in these paths as described below.)
   - (optional) Set upload or download permissions for this directory.
4. Save your settings (**File** > **Save Settings**).

Using variables in Directory Paths

The following pattern strings are available for configuring the **Local or UNC directory**. The resulting paths for Transfer Client users are shown here:

Default Home folder. For Web Edition users this is:

`C:\Users\<run_as_user>\ReflectionWebEdition\<domain_name>\<web_edition_user>`

This directory is created the first time a user logs into the Reflection for Secure IT Server if it doesn't already exist.

`%H` For Web Edition users this is equivalent to `%D`.

`%u` The user ID. This directory must already exist.

Caution: Do not use `%u` if you have users in multiple domains. If users in different domains have the same user ID, both users will have access to the same location. In this case, use `%U` (uppercase) to ensure unique pathnames.

`%U` The domain name and user ID in the format `domain.username`. This directory must already exist.

For Web Edition users who have been added to the default Reflection directory, the domain is `Reflection`. For example, for the external user whose UserID is "Mary":

```
c:\upload\%U
```

resolves to:

```
C:\upload\Reflection.Mary
```

Configure Access to Files on Back End SFTP Servers

The Transfer Client shows a **Local files** list on the left and a **Server files** list on the right. You can use the Reflection for Secure IT Server to add files to the **Server files** list that are located on one or more additional servers. Because these servers are not located on the host running Reflection for Secure IT, they are referred to as "remote servers" in the Reflection for Secure IT console. Because these remote file servers are frequently located behind your firewall, they are also referred to as "back end servers."

Note: This procedure configures access to files on an SFTP server. You can also configure access to files on a network share. See Configure Web Edition to Act as a Gateway (page 21).

To configure access to a directory on a back end SFTP server

1. On the Web Edition server, start the Reflection for Secure IT console (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**).
2. From the **Configuration** tab, click **SFTP Directories** in the left panel.

3 Click **Add** to open the **Accessible Directories Settings** dialog box.

4 Specify a **Virtual directory** name. This is the directory name users will see in the Transfer Client's **Server files** list.

5 Click **Remote SFTP server**. This opens the **Remote SFTP Server Connection** dialog box.

6 Specify a **Host** name.

7 Retrieve the host key.

8 Enter a username with access to this server for **Remote SFTP username**, and provide authentication information for this user.

9 In the **Path** field, enter a path on the server that the user has access to, or use **Browse** to have an available path entered for you.

10 Close the open dialog boxes and save the server settings.

Notes:

- The directories available on the remote server are limited by the rights of the user you specify for **Remote SFTP username**. You cannot provide access to files that are not available to this user.
- Users have access only to directories that you explicitly make available. They do not have access to other directories on the remote server, even if these directories are available to the specified **Remote SFTP username**.
- The `%u` and `%U` variables (page 37) are supported for specifying paths on remote servers.

Set File Upload and Download Permissions

In addition to configuring which files users have access to, you can also set permissions that determine what users can do with files.

Note: You can set different permissions for each virtual directory. By default these permissions apply to all users. You can use subconfigurations (page 39) to provide different permissions to specific users or groups of users.

To set file action permissions

1 On the Web Edition server, start the Reflection for Secure IT console (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**).

2 On the left panel of the **Configuration** tab, click **SFTP Directories**.

3 Click **Add** to create a new directory, or select an existing directory and click **Edit**.

4 Under **Permissions**, configure the access you want to allow. For example, to allow users to view and download files, but disallow any changes to the server files, leave **Browse** and **Download** checked, and clear **Upload**, **Delete**, and **Rename**.

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

The following permission options are available:

Browse	View file and directory lists.
Download	View file contents.
Upload	Modify files, create files, create directories, and modify file attributes.
Delete	Delete files and directories.
Rename	Rename files and directories.

Customize Group and User Settings

Using the Reflection for Secure IT console, you can customize file access and transfer rights for users and groups who have been provisioned using the Web Edition User Manager.

- To make customizations for users who have been added to the built-in Reflection directory, use the domain name `Reflection`.
- To make customizations for users in an added LDAP server, use the **Domain name** you specified when you added the LDAP server to User Manager (page 29).

The general procedures are outlined below. For a specific example, see Set Transfer Permissions for a User Group (page 24).

To create a subconfiguration with custom transfer settings for a user or group

1. From the **Configuration** tab of the Reflection for Secure IT console, click either **Group Configuration** or **User Configuration**.
2. For the group or user type, select **Domain**.

   For groups or users in the built-in Reflection directory, specify `Reflection` for the domain name.

   For groups and users in an added LDAP Server, specify the domain name for that server.
3. Enter the name of the user or group you want to customize.
4. Click any of the available options on the left side of the subconfiguration dialog box to configure options that will be applied to the specified user or group.
5. Click **OK** to close the open dialog boxes.
6. Save your settings (**File** > **Save Settings**).

To control server access for a user or group

1. From the Configuration tab of the Reflection for Secure IT console, click either **Group Access Control** or **User Access Control**.

2. Click **Add** and enter the user or group name using the following format, replacing *<name>* with the user or group name.

   `<domain>/<name>`

3. Specify the access setting for this user or group (allow or deny) and click **OK**.

   For information about how allow and deny settings affect user access, see the Reflection for Secure IT help topics "Controlling Access by User" and "Controlling Access by Group."

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

Set up File Transfer Auditing

You can use audit logging to maintain a record of file transfer activity. Audit logging is not enabled by default.

To enable file transfer auditing

1. On the Web Edition server, start the Reflection for Secure IT console (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**).

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, Reflection for Secure IT 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.

Start and Stop the Reflection for Secure IT Server

The Reflection for Secure IT Server is the SSH server application that supports secure file transfer. This server 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 Reflection for Secure IT Server console

1. On the Web Edition server, start the Reflection for Secure IT console (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**).

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

To use the Windows Services console

1. Log on to the Web Edition server (the computer on which you installed the Reflection for Secure IT SSH and Web Transfer servers).
2. Open the Windows Services console (**Start** > **All Programs** > **Administrative Tools** > **Services**).
3. Select the service called "Attachmate Reflection for Secure IT Server" and click start, stop, or restart.

CHAPTER 5

Web Transfer Server Administration

In this Chapter

The Reflection for Secure IT Web Transfer Server authenticates Web Edition users and is the application server that provides the Reflection for Secure IT Transfer Client.

Connect to the Transfer Client

The Reflection for Secure IT Web Edition Transfer Client is a web-based application. Access is available to any user who has been provisioned using the Web Edition User Manager.

End users can connect to the Transfer Client from a browser running on any system with access to the Web Edition Server that is running the Reflection for Secure IT Web Edition Web Transfer service:

To connect from a browser

- Enter the following URL, replacing <host> with the DNS name or IP address of your Web Edition host.

  ```
  https://<host>:9492
  ```

The Reflection for Secure IT Web Edition administrator can also connect to the Transfer Client from the Windows Start menu on the Web Edition server that is running the Reflection for Secure IT Web Edition Web Transfer service:

To connect from the Windows Start menu on the Web Edition server

- Go to **Start** > **All Programs** > **Attachmate Reflection** > **Web Edition Transfer Client**.

Start and Stop the Web Transfer Server

The Reflection for Secure IT Web Transfer Server is the application server that provides the Reflection for Secure IT Transfer Client. 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 Attachmate Reflection for Secure IT Web Transfer service

1 Log on to the Web Edition server (the computer on which you installed the Reflection for Secure IT SSH and Web Transfer servers).

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

3 Select the service called "Attachmate Reflection for Secure IT Web Transfer" and click start ,stop, or restart.

Note: After the service has started, it may take several seconds before the Transfer Client is accessible.

Customize the Look of the Transfer Client Web Pages

By default, the Transfer Client uses Attachmate Reflection for Secure IT branding. You can modify these web pages so that Transfer Client users see a page title and images that identify your organization.

To customize the Transfer Client web pages

1 Create a folder called `custom` in the `webapps` folder:

```
<install path>\WebTransfer\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 and create appropriate images as defined in this file, and replace the sample images provided with your images.

5 Connect to the Transfer Client or refresh the browser display to view the changes.

Web Transfer Server Properties File

You can use the Web Transfer properties file to modify the configurable settings listed below. It is located in the Web Edition installation folder in the `WebTransfer\conf` subfolder. The default location is:

```
C:\Program
Files\Attachmate\RSecureWebEdition\WebTransfer\conf\container.properties
```

Notes:

- You must restart the server (page 32) 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.

java.minimum.version

The minimum required Java version for browsers running the Transfer Client applet. The default is 1.7.0_21.

servletengine.ssl.updateInterval

The interval for how often the Web Transfer Server checks for changes to authentication settings made in User Manager and queries User Manager 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 47). The path must be specified using forward slashes or escaped backslashes. For example:

```
C:/pathto/keystore
```

```
C:\\pathto\\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 Web Transfer Server to connect to the Reflection for Secure IT Server. By default, the connection is made using the Reflection for Secure IT Server's computer name.

sftp.port

The port used by the Web Transfer Server to connect to the Reflection for Secure IT Server. The default is 22.

CHAPTER 6

Server Certificate Management

In this Chapter

Server Certificates

When you run the User Manager, the browser connects to the Reflection for Secure IT User Manager application server. When you run the Transfer Client, the browser connects to the Reflection for Secure IT Web Transfer Server. In both cases, the connection is made using HTTPS.

Why you see certificate warning messages

When an HTTPS connection is established, the browser requests that the server identify itself. By default, the Web Edition 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) (page 71). 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 Web Edition evaluation and configuration process, you may use any or all of the following 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 50).

  This option is appropriate during initial testing. You might also choose this as a permanent option for the User Manager.

- Replace the server's self-signed certificate with a certificate from a well-known Certificate Authority (page 47).

  Make this change to the Reflection for Secure IT Web Transfer Server before you provide end users with URLs for launching the Transfer Client. This change enables Transfer Client users to connect without seeing certificate warning messages.

Replace the Default Server Certificate

The following two Reflection for Secure IT Web Edition services install with self-signed digital certificates.

- Reflection for Secure IT Web Transfer service
- Reflection for Secure IT User Manager service

To be able to connect to the Transfer Client and User Manager without seeing certificate warning messages (page 46), you can replace the server's self-signed certificate 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 47)

Install a Server Certificate in a Java Keystore (page 48)

Install a New Server Certificate: PKCS#12 File

Use this procedure to replace the default Web Transfer or User Manager 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:

- The PKCS#12 private key and the store itself must use FIPS-compliant cryptography. PBE-SHA1-3DES is the only approved algorithm currently available for encrypting the store. (By default, OpenSSL and the Windows Certificate Manager do encrypt the store using this algorithm.) If your file is not FIPS-compliant, you can re-encrypt the PKCS#12 file (page 56) or import the file into a Java keystore (page 56).
- 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 PKCS#12 file (*.p12 or *.pfx)

The default install path is `C:\Program Files\Attachmate\RSecureWebEdition`.

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

```
C:\Program Files\Attachmate\RSecureWebEdition\WebTransfer\etc\

C:\Program Files\Attachmate\RSecureWebEdition\UserManager\etc\
```

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

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

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

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

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

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

servletengine.ssl.keystoretype=PKCS12

servletengine.ssl.keystorepassword=password
```

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

4 Restart the server you are configuring. See Start and Stop the Web Transfer Server (page 32) and Start and Stop the User Manager Server (page 32).

5 Test a connection from the Transfer Client or User Manager. . If you can't log in, or continue to see a certificate warning message, see Troubleshooting Server Certificate Setup (page 49).

Install a New Server Certificate: Java Keystore

Use this procedure to replace the default Web Transfer or User Manager 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 53),
- Create a Certificate Signing Request and submit it to a CA (page 54).
- Once you receive the signed certificate for your server, import the CA-signed certificate into your keystore (page 55).

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 another secure location on your server). The default keystore locations are:

```
C:\Program Files\Attachmate\RSecureWebEdition\WebTransfer\etc\
```

```
C:\Program Files\Attachmate\RSecureWebEdition\UserManager\etc\
```

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

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

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

```
<install path>\UserManager\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=password
```

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

4 Restart the server you are configuring. See Start and Stop the Web Transfer Server (page 32) and Start and Stop the User Manager Server (page 32).

5 Test a connection from the Transfer Client or User Manager. If you can't log in, or continue to see a certificate warning message, see Troubleshooting Server Certificate Setup (page 49).

Troubleshooting Server Certificate Setup

Refer to these troubleshooting steps if you changed the server certificate used by the Web Transfer or User Manager 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 Web Transfer Server (page 32) and Start and Stop the User Manager Server (page 32).

Error messages shown below are from the `console.`*`yyyymmdd`*`.log` (page 62) 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"

- 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 56) or import it into a Java keystore (page 56).

  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 after User Manager has been configured with a different certificate and before the Web Transfer Server has been updated to trust that certificate. To resolve this issue, from the Reflection for Secure IT console, go to the **Web Edition Users** pane and click **Activate and verify**.

Configure your Browser to Trust a Self-Signed Certificate

If you use the default Reflection for Secure IT certificates, you will see a certificate warning when you connect to the User Manager and the Transfer Client. Use these procedures to remove these warnings.

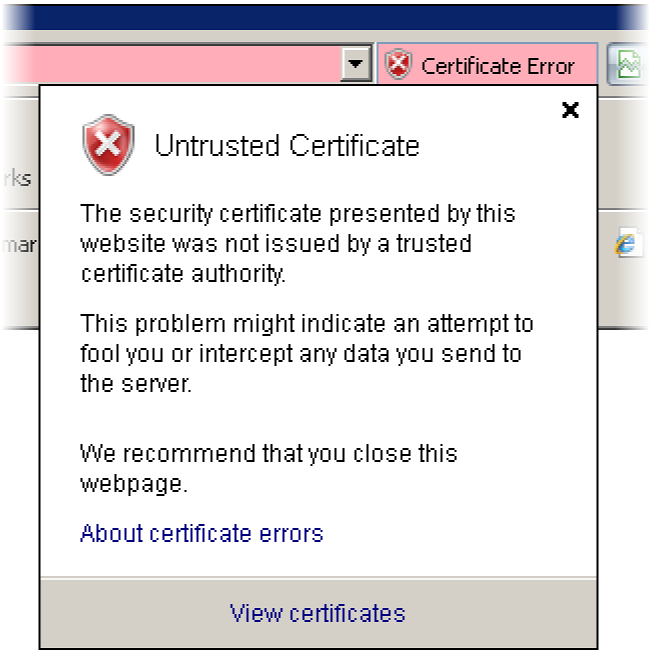
Note: The procedures below are appropriate for testing. However, before you deploy the Transfer Client to end users, you should configure Reflection for Secure IT to use certificates signed by a well-known Certificate Authority. (See Replace the Default Server Certificate (page 47).) With the updated 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:



Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

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.

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 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**.

2 Open the Windows certificate store:

- Click the customize button (three bars) in the upper right: ≡
- Click **Settings**.
- Click **Show advanced settings**.
- Click **Manage certificates**.

3 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 contained in a keystore. Depending on how you obtain certificates, you may use one or more of these procedures to manage your Reflection for Secure IT Web Edition 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

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 use a SET command to add this folder to your path as shown here.

   ```
   SET PATH=%PATH%;C:\Program Files\Common Files\Attachmate\JRE\1.7.0_21\bin
   ```

3. To review the available options, enter the following:

   ```
   keytool -help
   ```

Generate a Key Pair and Create a Keystore

This procedure uses the Java **keytool** (page 53) utility to generate a key and save it to a Java keystore.

Note: The CA you use may 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). For example:

   ```
   keytool -genkeypair -alias webedition -keyalg RSA -keysize 2048 -keystore
   newkeystore.jks -validity 365
   ```

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 Reflection for Secure IT Web Edition server (for example `webeditionhost.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'll 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.

Note:

If you use the keytool command as shown above, the utility prompts you to enter values for the items that make up the distinguished name (DN) in the certificate. An alternate option is to specify this value on the command line using the **-dname** option. For example:

```
keytool -genkeypair -dname "CN=webeditionhost.mycompany.com, O=My Company, C=US" -
alias webedition -keyalg RSA -keysize 2048 -keystore newkeystore.jks -validity
365
```

Create and Submit a Certificate Signing Request

This procedure uses the Java **keytool** (page 53) 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 53).

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:

   ```
   keytool -v -certreq -alias webedition -keystore newkeystore.jks -file
   cert_request.csr
   ```

2. Enter your keystore password when prompted.

3. You'll 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 the CA Certificate into your Keystore

This procedure uses the Java **keytool** (page 53) utility to import the CA-signed certificate into your existing keystore.

Before you begin

- You need a certificate for your server signed by a Certificate Authority.
- You need the trusted root CA certificate for the Certificate Authority.
- You need to know the keystore name, password, and alias you used when you created the keystore.

To import the CA certificate into your Java keystore with a CA-signed certificate

1. Use the `-importcert` option to 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 (`cacert` in this example); if the alias does not point to a key entry, **keytool** assumes you are adding a trusted certificate entry. For example:

   ```
   keytool -importcert -alias cacert -file CAcert.cer -keystore
   newkeystore.jks
   ```

   Note: Some CAs issue an intermediate certificate along with the main certificate. If this is true for your CA, then import these certificates using unique aliases to your keystore.

2 Use the `-importcert` option to add the server certificate you received from the CA (`certnew.cer` in this example) to your keystore. Use the alias you provided when you generated the keys; if the alias points to a key entry, **keytool** assumes you are importing a certificate reply. For example:

```
keytool -importcert -alias webedition -file certnew.cer -keystore
newkeystore.jks
```

Import a PKCS#12 File into a Java Keystore

This procedure uses the Java **keytool** (page 53) utility to create a Java keystore from a PKCS#12 file.

Before you begin

- You need a PKCS#12 (*.p12 or *.pfx) containing your CA-signed Web Edition 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 Web Edition 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.

```
SET PATH=%PATH%;C:\Program Files\Common Files\Attachmate\JRE\1.7.0_21\bin
```

3 Define a variable called `RWE_ROOT` that points to your Web Edition installation folder. For example, if you installed to the default location:

```
SET RWE_ROOT=C:\Program Files\Attachmate\RSecureWebEdition
```

4 Run the following command, replacing `nonfips.p12` and `fips.p12` with your source and destination filenames. (This should all be on one line. 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
"%RWE_ROOT%\UserManager\lib\cryptojce-
6.1.jar;%RWE_ROOT%\UserManager\lib\cryptojcommon-
6.1.jar;%RWE_ROOT%\UserManager\lib\jcmFIPS-6.1.jar" -importkeystore -
srcstoretype PKCS12 -srckeystore nonfips.p12 -destkeystore fips.p12 -
deststoretype PKCS12
```

CHAPTER 7

Troubleshooting

In this Chapter

Transfer Client Troubleshooting

The Browser Cannot Display the Web Page

The browser is unable to display the Transfer Client web page.

- Are the Reflection for Secure IT services running?

  If you just restarted your Windows computer or just started your User Manager or Web Transfer service, wait a minute and try again. These services take a few moments to become available.

  To confirm that the services are running, open the Windows Services console (**Start** > **All Programs** > **Administrative Tools** > **Services**).

  If the Transfer Client page can't be displayed, on the Web Edition system confirm that "Attachmate Reflection for Secure IT Web Transfer" is started.

  If the User Manager page can't be displayed, on the User Manager system confirm that "Attachmate Reflection for Secure IT User Manager" is started.

- Are required ports open in your firewall?

  For the Transfer Client, check that port 9492 is open inbound to the system running the Reflection for Secure IT Web Transfer Server.

  For the User Manager, check that port 9490 is open inbound to the system running the Reflection for Secure IT User Manager.

- Is the server certificate correctly configured?

  See Troubleshooting Server Certificate Setup (page 49).

Password Login Fails at the Transfer Client Login Page

The Transfer Client login page displays, but the user is unable to log in.

The users 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 User Manager?

  In User Manager, select the LDAP server, enter the UserId and click **Filter UserID** to confirm that the user exists in the database.

- If the user exists, is the password correct?

  If a Reflection directory user has forgotten the password, you can edit the user in User Manager to change the password.

- If the user is in an added LDAP server, has the user entered the correct credentials for their username on the LDAP server?

- If the user is in an added LDAP server and entered a username in the form `domain\user`, does the value for domain exactly match the **Domain Name** specified in User Manager?

  Connect to User Manager, click **LDAP Server**, select your server, click **Edi**t and check the value entered for **Domain Name**. If you specified `mydomain.com`, users must log using the format `mydomain.com\user`. Users will not be able to log in using the format `mydomain\user`.

The user sees an error message that says "Server not configured. Please contact your system administrator."

- Have configuration changes affected the connection between the Reflection for Secure IT Server and the User Manager?

  On the server running the Reflection for Secure IT Server, start the server console. On the **Web Edition Users** pane, click **Activate and verify.**

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 User Manager or Web Transfer service, wait a minute and try again. These services take a few moments to become available.

  To confirm that the services are running, open the Windows Services console (**Start** > **All Programs** > **Administrative Tools** > **Services**) and confirm that the Attachmate Reflection for Secure IT services are all running.

- Are required ports open in your firewall?

  Check that port 9490 is open inbound to the system running the Reflection for Secure IT User Manager.

- Have you made configuration changes that affect the connection between the Reflection for Secure IT Server and the User Manager? For example, you may see this error after upgrading to version 8.1 from an 8.0 installation that had been configured to use a non-default server certificate.

  On the server running the Reflection for Secure IT Server, start the server console. On the **Web Edition Users** pane, click **Activate and verify.**

For additional troubleshooting, refer to the log files (page 62) for each of the Web Edition servers.

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.

If no dialog box error message is displayed and "Connection failed: <User name>" appears in the menu bar next to the Logout button:

- Is the Reflection for Secure IT Server running?

  On the Web Edition server, open the Windows Services console (**Start** > **All Programs** > **Administrative Tools** > **Services**). Confirm that "Attachmate Reflection for Secure IT Server" is started.

- Is port 22 open inbound to the system running the Reflection for Secure IT Server?

If 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 this problem, start the Reflection for Secure IT console (**Start** > **All Programs** > **Attachmate Reflection** > **Reflection SSH Server Configuration**.

- Is support for Web Edition users enabled in the Reflection for Secure IT Server?

  Go to **Web Edition Users**. Is **Allow access to Web Edition users** enabled?

- Are the **Web Edition user access account** credentials valid?

  Go to the **Web Edition Users** pane, click **Select account**. Select the account name, click **Edit**, then click **Test**.

- Are server certificates or other Web Edition connection requirements correctly configured on the Reflection for Secure IT Server?

  On the **Web Edition 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 may have corrected the problem. You should retest. If the connection doesn't complete successfully, use the messages in the dialog box for additional troubleshooting.

- 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 Reflection for Secure IT Server log file (page 62).

If 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 Reflection for Secure IT log file (page 62) 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 Transfer Fails

The user makes a successful connection to the Transfer Client but is unable to transfer files.

The user sees an error message that says, "File <filename> transfer failed."

- Have transfer rights been disabled in the Reflection for Secure IT Server?

  In the **SFTP Accessible Directories Settings** dialog box, look at the **Permissions** settings.

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?"

- Has upload access been disabled in the **SFTP Accessible Directories Settings** dialog box under **Permissions?**
- Does the **Web Edition user access account** have access to the **Local or UNC directory** specified in the **SFTP Accessible Directories Settings** dialog box?
- Does the user you specified in the **Remote SFTP Server Configuration** dialog box for **Remote SFTP username** have rights to the path specified on the remote server? Use the **Browse** button to ensure that you specify an available directory.

Note: In all of the above cases, no remote file is created, so clicking Yes and No are equivalent in response to "Would you like to delete the remote file?

The user sees an error message that says, "Failed to change to remote directory <directory name>."

- Does the directory exist?

  Note: If you use %u or %U in a directory path, you must create user directories in advance; these directories are not created automatically when the user logs in.

- Is the password specified for the remote SFTP user correct? Or, if public keys are specified, is public key authentication correctly configured?

The user sees an error message that says, "Unable to execute the file transfer request. The remote directory "<directory name>" does not exist.

- Does the directory specified as the user home directory exist on the Reflection for Secure IT Server?

Certificate Authentication Fails

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 User Manager is configured to require authentication using X.509 certificates and authentication is not successful.

- PKI Services Manager is not running or is not correctly configured in the User Manager.

  Try testing the connection to PKI Services Manager from User Manager. Go to **Configuration** > **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 User Manager.

- The certificate is valid, but PKI Services Manager is not correctly configured to validate it.

  See "Troubleshooting PKI Services Manager Configuration" in the PKI Services Manager User Guide, which is available from http://support.attachmate.com/manuals/pki.html.

- 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.

Log Files

User Manager and Web Transfer Logs

Log files for the User Manager and Web Transfer Server are created in the `logs` folders:

```
<install path>\UserManager\logs
```

```
<install path>\WebTransfer\logs
```

Logging configuration can be modified using `logback.xml` or `container.conf`, depending on which log you want to modify. Instructions are provided in these files.

Note: Edits you make to `logback.xml` and `container.conf` need to be repeated each time you apply a hotfix or upgrade your Reflection for Secure IT software.

The files are located in the conf folders:

<*install path*>\UserManager\conf

<*install path*>\WebTransfer\conf

The following log files are available for both the Web Transfer Server and the User Manager:

server.log
server.*yyyymmdd*.log

The server log includes primary server logging. 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.

To modify the server log settings, use logback.xml.

console.*yyyymmdd*.log

The console log has startup and runtime details. 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.

debug.log

Debug logging is not enabled by default. A debug.log file is created by default, but is not used 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 User Manager:

directory.log

The directory log contains logging related to LDAP directory transactions. Rollover configuration is the same as the server log, however rolled over logs are usually not present. Rollover is triggered when messages are written to the log files, and this log is rarely used.

To modify the directory log settings, use logback.xml.

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.

Reflection for Secure IT Server Logs

The Reflection for Secure IT Server supports two methods of logging: to the Windows Event Viewer and/or to a text log file. To configure logging, use the Reflection for Secure IT console (**Attachmate Reflection** > **Reflection SSH Server Configuration**).

Windows Event Viewer

Logging to the Event Viewer is enabled by default.

To view the Event Viewer log from the Reflection for Secure IT 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 Reflection for Secure IT console, click the toolbar button, or go to **View** > **Latest Debug Log File**.

Managing Text File Line Endings

File transfers between the Web Edition Transfer Client and the Reflection for Secure IT 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 Reflection for Secure IT Server 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 Reflection for Secure IT servers; it will not work with OpenSSH servers.)

For transfers involving all three systems (the Transfer Client, the Reflection for Secure IT Server, and a remote SFTP server) where text conversion is configured and working on the Reflection for Secure IT Server:

- All files exposed by the Reflection for Secure IT Server for download will have Windows line endings.
- The Reflection for Secure IT Server expects all uploaded files to have Windows line endings.

CHAPTER 8

Supplemental Administrative Topics

In this Chapter

Security Recommendations for the Web Edition Server

Use the following precautions to help ensure security on the system running the Reflection for Secure IT Server and the Reflection for Secure IT Web 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 Reflection for Secure IT Server console, on the **Web Edition Users** pane leave **Restrict Web Edition users to file transfer sessions** selected. This default setting helps minimize external user access to your system. Also, disable port forwarding for all users. To do this, clear both port forwarding options on the **Permissions** pane under **Tunneling**.
- Configure firewalls (page 12) that limit access to ports on your servers.

Reflection for Secure IT Web Edition 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.

User Manager

These User Manager data files are located in the Web Edition installation folder (`C:\Program Files\Attachmate\RSecureWebEdition` by default). User Manager can be on the same computer that runs the Reflection for Secure IT Server and Reflection for Secure IT Web Transfer Server, or another computer.

Directory	Data description
`\UserManager\services\directory\data\`	Reflection LDAP directory data. This directory contains user information, including hashed passwords.
`\UserManager\services\peermgmt\data\`	Reflection LDAP directory data
`\UserManager\etc\`	User Manager certificates
	Caution: Do not delete any of the existing certificate or keystore files in these locations. The server certificates located here are required for communication between Web Edition components. Deleting the User Manager's server keystore and certificate will cause authentication of LDAP users to fail. If your User Manager Administrators group consists entirely of users in remote LDAP directories, you will no longer be able to log in to User Manager.
`\UserManager\conf\container.properties`	User Manager settings

Web Transfer Server

These Web Transfer Server data files are located in the Web Edition installation directory (`C:\Program Files\Attachmate\RSecureWebEdition` by default).

Directory	Data description
`\WebTransfer\etc\`	Web Transfer Server certificates Caution: Do not delete any of the existing certificate or keystore files in these locations. The server certificates located here are required for communication between Web Edition components.
`\WebTransfer\conf\container.properties`	Web Transfer Server settings

Reflection for Secure IT Server

Directory	Data description
`C:\ProgramData\Attachmate\RSecureServer\`	Reflection for Secure IT Server settings, server certificates, key files, and the credential cache.

Copy Data to a New Server

You can use this procedure to copy data from an earlier version of Reflection for Secure IT Web Edition or to restore data from backup files. Data files can be copied over to newly installed servers either before or after the old servers are upgraded or uninstalled.

To copy data to a new server

1. Install Reflection for Secure IT Web Edition on the new server.
2. Restart the new server (or start the services), which will create default folders and files.
3. Stop the services on the new server.
4. Delete the default data files on the new server.
5. Stop the services on the original server.
6. Copy the data files (page 66) from the old server to the new server.
7. Start the services on the new server.
8. Optionally uninstall or upgrade the old server.

Changing the JRE

Use the procedures below to configure the Web Transfer Server and User Manager to use a different Java Runtime Environment (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 Reflection for Secure IT Web Edition or apply a hotfix, you need to repeat the changes to the properties files.

Apply the Unlimited Strength Jurisdiction Policy Files to your JRE

1. Go to the Java SE Downloads page.
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. Replace the existing limited strength policy files (located in `<java-home>\jre\lib\security`) with the unlimited strength policy files. For example:

   ```
   C:\Program Files\Java\jdk1.7.0_25\jre\lib\security
   ```

Note: You need to repeat this procedure each time you upgrade your JRE. If you use automatic updates, JRE updates will continue to use the same default folder (`C:\Program Files\Java\jre7`), and each new version will overwrite any changes you made to the prior version. Java Development Kit (JDK) updates, which include the JRE, use a different folder for each update (for example `C:\Program Files\Java\jdk1.7.0_25`).

Edit the properties files and restart the servers

1. Locate the configuration properties file (`container.conf`) for both the User Manager and the Web Transfer Server:

   ```
   <install path>\UserManager\conf\container.conf
   ```

   ```
   <install path>\WebTransfer\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_25\bin\java
   ```

3. Restart both servers. (page 32, page 43)

Note: You need to repeat this procedure each time you upgrade Reflection for Secure IT Web Edition or apply a hotfix.

Set Up PKI Services Manager

Reflection PKI Services Manager is a service that provides certificate validation services. If your client users will authenticate using X.509 certificates, you need to install and configure this service. It is available at no additional charge from the Reflection for Secure IT Web Edition download page. Reflection for Secure IT Web Edition requires version 1.2 SP2 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 User Manager 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. 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. 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 Web Edition, your mapping configuration must return a single allowed user 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 in 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 user who can log in 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.
`{ %subst% } Subject.CN Regex [a-zA-Z\.]*([0-9]+)`	The allowed user name is equal to the first numerical string within the common name portion of the Subject field. For example, if the CN is "joe.smith.12345", the allowed identity is set to "12345".

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 Web Edition 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.

```
{ root dgreen } Subject.Email Equals donald.green@acme.com
```

Note: Rules that configure multiple allowed identities for a single certificate are valid for SSH connections. For example, you can use a rule like the one above if you are configuring PKI Services Manager to validate certificates for users logging directly into the Reflection for Secure IT Server. In this case the user has already provided a username and the mapping rule establishes a set of one or more permitted names. Authentication is successful if the presented username is included within that set. In the case of an SSL connection (such as the connection to the Transfer Client), the user presents a certificate without a username and the mapping rules must return the username for exactly one user who can authenticate with this certificate.

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 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.

P

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. 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

X.509 certificate

See digital certificate (page 71).

Index