

Reflection for Secure IT Gateway Administrator's Guide

Version 1.1 SP2

Legal

Legal Notice

© Copyright 2019 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contains Confidential Information. Except as specifically indicated otherwise, a valid license is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Contents

| | |
|--|-----------|
| Reflection for Secure IT Gateway | 7 |
| 1 Introduction | 9 |
| Jobs | 9 |
| Transfer Sites | 9 |
| Job Components | 10 |
| Transfer Site Components | 12 |
| Comparing Jobs and Transfer Sites | 14 |
| Reflection for Secure IT Gateway Architecture | 15 |
| 2 Installation and System Requirements | 17 |
| Server System Requirements | 17 |
| Transfer Client Requirements | 18 |
| Reflection for Secure IT Gateway Components | 18 |
| Installing Reflection Gateway | 19 |
| Ports and Firewall Configuration | 21 |
| 3 Initial Configuration | 25 |
| Initial Configuration Steps for Using Jobs | 25 |
| Initial Configuration Steps for Using Transfer Sites | 25 |
| How To... | 26 |
| Log on to the Gateway Administrator | 26 |
| Add File Servers to Gateway Administrator | 27 |
| Set Up Directory Access on your SFTP Servers | 29 |
| Add Hubs to Gateway Administrator | 30 |
| Configure Email Support in Gateway Administrator | 30 |
| Enable Reflection Gateway Connections in the Reflection Secure Shell Proxy | 32 |
| Set Up the Transfer Site File Server | 33 |
| Configure Server Certificates | 34 |
| 4 Managing Users and Groups | 35 |
| Add Users to the Default User List | 35 |
| Delete or Disable Users | 36 |
| Provision Users from an Added LDAP Server | 37 |
| Add LDAP Users to the Administrators Group | 39 |
| LDAP Server Advanced Domain Settings | 40 |
| Creating and Editing Groups | 42 |
| Roles in Reflection Gateway | 43 |
| Configure Certificate User Authentication | 44 |
| Set Up PKI Services Manager | 45 |
| 5 Managing Jobs | 47 |
| How to Create and Test Jobs | 47 |
| Connect to Gateway Administrator | 48 |

| | |
|---|-----------|
| Create a Job | 48 |
| Configure a Job Action that Transfers Files | 50 |
| Configure a Job Action that Executes a Command | 52 |
| Notes for Testing Job Actions | 54 |
| Job Tokens | 55 |
| Tokens for Job Actions that Transfer Files | 55 |
| Tokens for Job Actions that Execute Commands | 55 |
| 6 Managing Transfer Sites | 57 |
| How to Create Transfer Sites and Transfer Files | 58 |
| Connect to Gateway Administrator | 58 |
| Create a Transfer Site | 58 |
| Start the Transfer Client | 60 |
| The Transfer Client User Interface | 61 |
| Use Quick Add to Add Transfer Sites and Users | 62 |
| Transfer Files using an Alternate SFTP Client | 63 |
| Post Transfer Actions | 64 |
| Configure Post Transfer Actions in Gateway Administrator | 65 |
| Configure Post Transfer Actions in Reflection for Secure IT | 68 |
| Post Transfer Action Tokens | 70 |
| 7 Gateway Administrator User Interface | 73 |
| Transfer Sites | 73 |
| New/Edit Transfer Site | 74 |
| Jobs | 76 |
| New/Edit Job | 77 |
| Transfer File (Job Action) | 78 |
| Execute Command (Job Action) | 79 |
| Users | 80 |
| New User | 81 |
| Edit User | 82 |
| Groups | 82 |
| New Group | 83 |
| Edit Group | 83 |
| Add Members | 84 |
| Actions | 84 |
| New/Edit Action | 85 |
| System | 85 |
| LDAP Servers Tab | 86 |
| Email Server Tab | 88 |
| Email Templates Tab | 89 |
| File Servers Tab | 90 |
| File Server Groups Tab | 92 |
| Hubs Tab | 93 |
| Authentication Tab | 94 |
| PKI Servers Tab | 95 |
| 8 Troubleshooting | 97 |
| Log Files | 97 |
| Gateway Administrator, Hub, and Transfer Server Logs | 97 |
| Add Debug Logging to the Server Log File | 98 |
| Reflection Secure Shell Proxy Logs | 98 |
| SFTP File Server Configuration Troubleshooting | 99 |
| Hub Configuration Troubleshooting | 99 |
| Job Troubleshooting | 100 |

| | |
|--|-----|
| Transfer Client Troubleshooting | 101 |
| The Browser Cannot Display the Web Page | 102 |
| Password Login Fails at the Transfer Client Login Page | 102 |
| Transfer Client Login Succeeds but the Server Connection Fails | 103 |
| Server Connection Succeeds but the Transfer Fails | 104 |
| Certificate Authentication Fails | 105 |
| Managing Text File Line Endings | 106 |
| Password Troubleshooting | 106 |
| Gateway Administrator Login Page Troubleshooting | 107 |
| Email Troubleshooting | 107 |
| Post Transfer Action Troubleshooting | 108 |
| Server Certificate Troubleshooting | 109 |

9 Reflection Gateway System Administration 111

| | |
|---|-----|
| Email Administration | 111 |
| Initial Email Setup | 111 |
| Transfer Site Email Notifications | 112 |
| Customize Transfer Site Email Templates | 113 |
| Transfer Site Email Tokens | 114 |
| Configuration and Data Files | 116 |
| Gateway Administrator Properties File | 117 |
| Transfer Server Properties File | 119 |
| Hub Properties File | 120 |
| Reflection Gateway Data Files | 121 |
| Backing Up Gateway Administrator Data | 123 |
| Changing the Gateway Administrator Database | 123 |
| Job Administrative Topics | 125 |
| Configure Preset Actions and Email Notifications using a Job Template | 125 |
| How Reflection Gateway Determines if Files have Changed. | 126 |
| Transfer Site Administrative Topics | 127 |
| Change the Transfer Site Directory used by the Reflection Secure Shell Proxy | 127 |
| Use an Added SFTP Server as the Transfer Site File Server | 128 |
| Configure Connections to Remote SFTP Servers from the Reflection Secure Shell Proxy | 128 |
| Customize the Look of the Transfer Client Web Pages | 130 |
| Security Recommendations for the Reflection Secure Shell Proxy | 130 |
| Server Certificate Management | 131 |
| Replace the Default Server Certificate | 131 |
| Configure Your Browser to Trust a Self-Signed Certificate | 134 |
| Migrate PKCS#12 or JCEKS keystores to BCFKS keystores | 135 |
| Using the Keytool Utility to Manage Keystores | 136 |
| Managing the Reflection Gateway Services | 140 |
| Start and Stop the Reflection Gateway Administrator Service | 140 |
| Start and Stop the Reflection Transfer Server | 140 |
| Start and Stop the Reflection Hub | 141 |
| Reset Server Authentication on a Reflection Hub | 141 |
| Start and Stop the Reflection Secure Shell Proxy | 141 |
| Reset Gateway Administrator to All Defaults | 142 |
| Ensuring High Availability of Reflection Gateway Services | 143 |
| Configure Duplicate Gateway Administrator Systems | 145 |
| Configure Duplicate Reflection Gateway Proxy Systems | 147 |
| Sample HAProxy Configuration | 149 |
| Create an Audit Log of File Transfers | 150 |
| Change the JDK | 151 |

Glossary of Terms 153

Reflection for Secure IT Gateway

Reflection for Secure IT Gateway provides a secure, flexible way to manage files. Reflection Gateway offers two key features: Jobs and Transfer Sites. Both use secure authentication and encryption for all connections and provide administrators with flexible options for creating custom configurations appropriate to different users and business practices.

This guide provides information for the system administrators who will do initial installation and setup and also for users who will manage Jobs and Transfer sites after initial setup is complete.

- ◆ [Chapter 1, “Introduction,” on page 9](#)
- ◆ [Chapter 2, “Installation and System Requirements,” on page 17](#)
- ◆ [Chapter 3, “Initial Configuration,” on page 25](#)
- ◆ [Chapter 4, “Managing Users and Groups,” on page 35](#)
- ◆ [Chapter 5, “Managing Jobs,” on page 47](#)
- ◆ [Chapter 6, “Managing Transfer Sites,” on page 57](#)
- ◆ [Chapter 7, “Gateway Administrator User Interface,” on page 73](#)
- ◆ [Chapter 8, “Troubleshooting,” on page 97](#)
- ◆ [Chapter 9, “Reflection Gateway System Administration,” on page 111](#)
- ◆ [“Glossary of Terms” on page 153](#)

1 Introduction

- ◆ “Jobs” on page 9
- ◆ “Transfer Sites” on page 9
- ◆ “Job Components” on page 10
- ◆ “Transfer Site Components” on page 12
- ◆ “Comparing Jobs and Transfer Sites” on page 14
- ◆ “Reflection for Secure IT Gateway Architecture” on page 15

Jobs

Use Jobs to configure secure, automated handling of files. Reflection Gateway monitors the content of a directory and initiates an ordered sequence of events when it finds new files or updated files in the scanned directory. Changed files can be the result of Transfer Site uploads or any other process that moves and modifies files.

Job Features

- Monitor directories on any added SFTP file server.
- Create a customized, ordered sequence of Job actions to handle new and updated files. Actions can include:
 - ◆ Moving or copying files to any added server.
 - ◆ Executing any command supported on the server where files first arrive, or on subsequent servers to which files are moved. For example, you can use system commands to delete or rename files, or run a command-line executable such as a virus scanner.
- If any action in your sequence fails, no further actions take place. This ensures that the processes you configure to secure your site are successfully completed on all files.
- Configure email notification to alert system administrators when Job actions fail or succeed.
- Specify which directory to scan and whether or not to include subdirectories.
- Define the window of time that the directory will be monitored. For example, Monday through Friday from 8 AM to 5 PM.
- Set the scan interval to determine how frequently scans occur, for example every 30 minutes.
- Specify which files in the directory should be acted on, for example all PDF files, or all files of a given size.
- Specify the minimum number of files that must arrive before Job actions begin.
- Set up File Server Groups to enable users to configure Jobs only on specific file servers.

Transfer Sites

Use Transfer Sites to configure secure file exchange with business partners and employees working outside your corporate network. User authentication is required for all transfers and end-to-end encryption protects all transferred data.

Transfer Site Features

- ◆ Integrated web-based Transfer Client

This web-based client provides an easy drag-and-drop interface for transferring files or entire directories. You can customize the Transfer Client to use branding and images that identify your organization.

NOTE: Using the Reflection Transfer Client to access Transfer Sites is not a requirement. Reflection Gateway users can also use the Reflection for Secure IT Secure Shell client, the Reflection FTP Client configured for SFTP transfer, or any other SFTP-enabled SSH client.

- ◆ End-to-end encryption

All transfers are securely encrypted. In addition, when you set up a back-end Transfer Site file server, encrypted data streams continuously through the Reflection Gateway Proxy, eliminating the need to save files on the proxy. This is more secure and more efficient than file transfer solutions that require the file to be stored and then forwarded.

- ◆ Configurable Transfer Site access

Transfer site managers can provide access rights to users or groups and control how long sites remain active. Permissions settings are available to specify who can upload and/or download files and who receives email notifications.

- ◆ Self-registration by email

New external users can be notified via email with links provided for password creation. Customizable email templates are available for account creation, password reset, Transfer Site access notifications, and file upload and download notifications.

- ◆ Manage files after a transfer

You can use either Post Transfer Actions or Jobs to trigger automated processes after files are uploaded to your server. See [“Comparing Jobs and Transfer Sites” on page 14](#).

- ◆ File Transfer auditing

Use audit logging to maintain a complete record of all file transfer activity.

Job Components

Jobs enable you to automate the secure transfer and handling of files. Reflection Gateway scans for new and updated files in specified directories located on any [added SFTP server \(page 27\)](#).

The main components for Job actions are:

- ◆ **Reflection Gateway Administrator**

The Reflection Gateway Administrator service is the central management service for Reflection Gateway. It interacts with other Reflection Gateway components and provides a web user interface. For Job setup, you will use it to manage user and groups access, add connection information for your SFTP servers, add connection information for and the server(s) running the Reflection Hub service, configure scan intervals and filters, and set up Job actions. Configuration data is stored on a database. You can use the default database, which runs on the same server, or configure Gateway Administrator to use an alternate database.

- ◆ **Reflection Hub**

The Reflection Hub service makes connections to SFTP servers and executes the Job actions you have defined using Gateway Administrator. You can configure multiple Hubs to help ensure high availability and rapid response. Each Hub communicates with Gateway Administrator

securely using HTTPS. Certificate authentication for these connections is configured when you add the Hub to Gateway Administrator. Hubs communicate with SFTP servers using secure SFTP connections. Authentication for these connections is configured when you add the SFTP server to Gateway Administrator.

◆ **SFTP servers**

You can configure Reflection Gateway to scan files on any SFTP server you have added using Gateway Administrator. You can transfer files to and from the scanned server, and any other added SFTP server. You can also manage your files by executing commands on any added server.

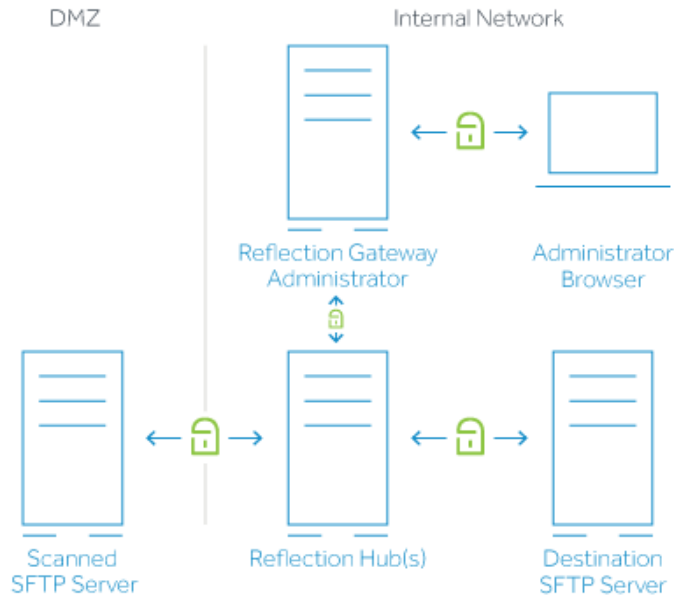
NOTE: The diagrams in this section show only the components required for Jobs. If you are setting up for both Jobs and Transfer Sites, review [“Reflection for Secure IT Gateway Components”](#) on [page 18](#) to see how to include Transfer Site components in your planning.

You can install all Reflection Gateway services on a single server or use a distributed configuration.

For example, the configuration shown below installs the Reflection Gateway Administrator and Reflection Hub services on a single system. The administrator can launch the Gateway Administrator web application directly from this system. This sample configuration uses two SFTP servers. One server is scanned for new or updated files. Job actions can be configured to act on the arriving files and transfer them to the second SFTP server. A configuration like this can be helpful for initial testing even if your final plans involve a more complex configuration.



An example of a more distributed configuration is shown below.



Related Topics

- ◆ [“Reflection for Secure IT Gateway Components” on page 18](#)
- ◆ [“Transfer Site Components” on page 12](#)
- ◆ [“Installing Reflection Gateway” on page 19](#)
- ◆ [“Initial Configuration” on page 25](#)

Transfer Site Components

Transfer Sites provide a secure way to manage file exchange. Secure authentication and encryption are used for all connections.

The main components for Transfer Sites are:

- ◆ **User workstation**

Users can transfer files using the web-based Reflection Transfer Client or an alternate SFTP client.

- ◆ **Reflection Gateway Proxy**

The following two services always run on the same server. These services are installed together when you install the Reflection Gateway Proxy feature.

- ◆ **Reflection Transfer Server:** Provides the Transfer Client web application and communicates with the Reflection Gateway Administrator for user authentication and Transfer Site configuration information.
- ◆ **Reflection Secure Shell Proxy:** Manages Secure Shell file transfers to and from the designated Transfer Site file server.

- ◆ **Reflection Gateway Administrator**

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

- ◆ **Transfer Site file server**

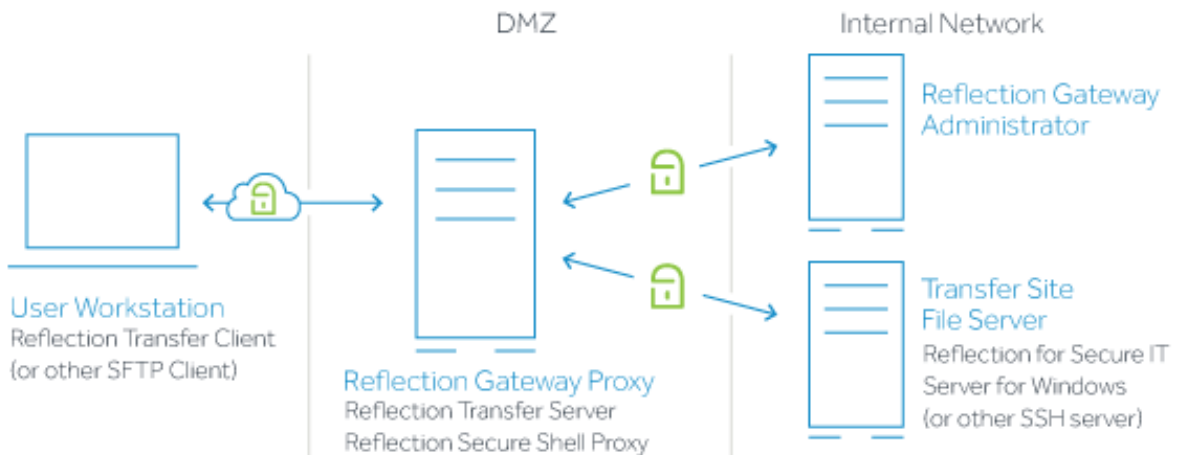
In the simplest configuration, you upload and download files to and from the Reflection Gateway Proxy. However, in most cases you will want to store files securely behind your firewall. You can configure to transfer files to and from a designated file server. This can be a Windows system running the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

NOTE: The configuration diagrams in this section show only the components required for Transfer Sites. If you are setting up for both Jobs and Transfer Sites, review [“Reflection for Secure IT Gateway Components” on page 18](#) to see how to include Job components in your planning.

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



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



Related Topics

- ◆ [“Reflection for Secure IT Gateway Components” on page 18](#)
- ◆ [“Job Components” on page 10](#)
- ◆ [“Installing Reflection Gateway” on page 19](#)
- ◆ [“Initial Configuration” on page 25](#)

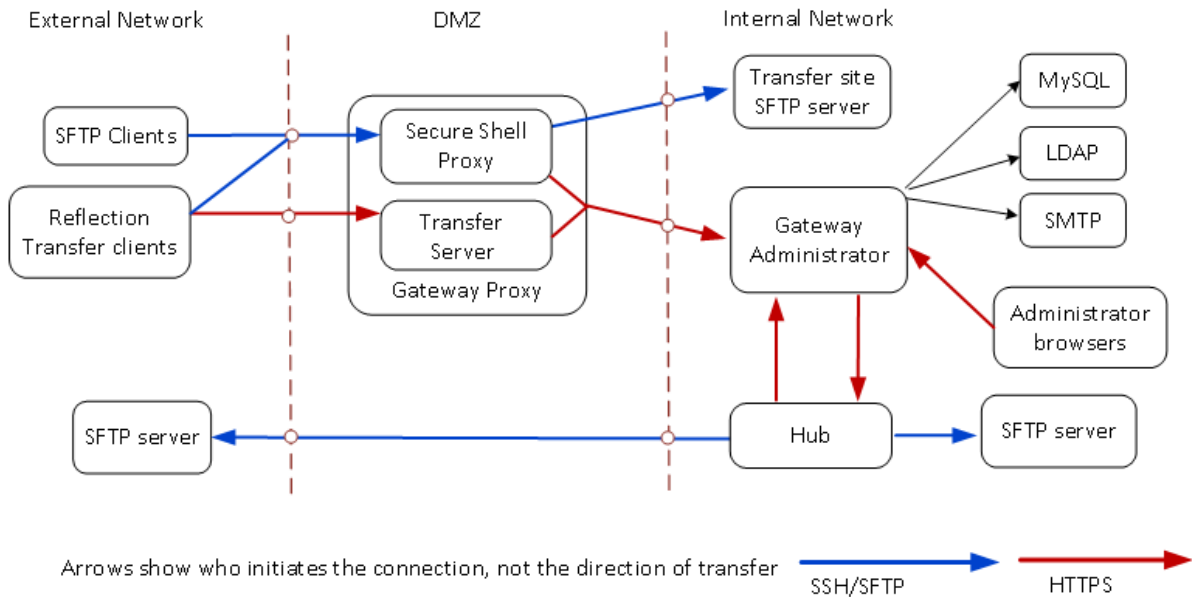
Comparing Jobs and Transfer Sites

Use this table to help you plan how to use Jobs and Transfer Sites to best manage files in your environment.

| Job | Transfer Site |
|--|--|
| Transfers and/ or command actions are initiated automatically when new or updated files appear in a specified directory. | Transfers are initiated by users. |
| You can configure transfers to take place between any SFTP servers that have been added to Gateway Administrator. | All files are transferred to and from a single designated Transfer Site file server. |
| You can configure any sequence of transfers and command actions, and control what sequence the actions occur in. If any action in the sequence fails, subsequent actions are not executed. | You can configure one or more Post Transfer Actions to take place after a successful upload. Although you can configure multiple actions, you cannot control the sequence or interrupt the sequence after a failure. |
| Jobs are triggered at a specified scan interval; actions do not take place immediately when a file arrives in a scanned directory. | Post Transfer Actions take place as soon as a file is uploaded to a Transfer Site. |
| Each Job is configured independently. You can use the Job copy feature to create similar actions in different Jobs. | The same Post Transfer Action can be added to multiple Transfers Sites. |
| NOTE: You can combine Transfer Sites and Jobs. For example, if you want uploads to a Transfer Site to trigger a sequence of events, you can create a Job that monitors the directory used by the Transfer Site. | |

Reflection for Secure IT Gateway Architecture

The diagram and table below summarize the components of a Reflection Gateway installation.



| Component | Description |
|-----------------------|--|
| Transfer Client | Required for Transfer Sites |
| SFTP client | Transfer Site users can transfer files using either the web-based Reflection Transfer Client (page 60) or any alternate SFTP client (page 63) that is available on their system. |
| Gateway Proxy | Required for Transfer Sites. Not used by Jobs The Gateway Proxy system runs two services that must be installed together—the Reflection Transfer Server and the Reflection Secure Shell Proxy. |
| Gateway Administrator | Required for all Reflection Gateway installations. Provides an HTML based configuration UI, provides web services to authenticate users and provides access to data. Also interfaces with existing LDAP, MySQL and Email servers. |
| Reflection Hub | Required for Jobs. Not used by Transfer Sites. Makes connections to SFTP servers and executes the Job actions defined in the Gateway Administrator. |
| SFTP servers | Required for Jobs. Optional for Transfer Sites. Configure connections to one or more SFTP servers (page 27) . Jobs and Transfer sites can use the same server or different servers. No added SFTP server is required for Transfer Sites if you use the Reflection Gateway Proxy as the Transfer Site file server. The Reflection for Secure IT Gateway installer includes the Reflection for Secure IT Server for Windows. Each Reflection Gateway license entitles you to install this SFTP-enabled server on one system. |

| Component | Description |
|-------------------|---|
| MySQL database | Optional Gateway Administrator installs and uses a HyperSQL database by default. The default database is created on the same system as Gateway Administrator. For production environments that require high availability, configure Gateway Administrator to use a MySQL database (page 123) , which can run on a remote server. |
| LDAP directory | Optional In addition to adding users to the built-in ReflectionGateway list, you can provide users with access to Transfer Sites or the Gateway Administrator by configuring user authentication from an external LDAP directory |
| SMTP email server | Optional Email notifications are commonly used in both Jobs and Transfer Sites. To support this, configure Gateway Administrator to connect to an email server (page 30) . |

Related Topics

- ◆ [“Installing Reflection Gateway” on page 19](#)
- ◆ [“Initial Configuration” on page 25](#)
- ◆ [“Ports and Firewall Configuration” on page 21](#)

2 Installation and System Requirements

- ◆ “Server System Requirements” on page 17
- ◆ “Transfer Client Requirements” on page 18
- ◆ “Reflection for Secure IT Gateway Components” on page 18
- ◆ “Installing Reflection Gateway” on page 19
- ◆ “Ports and Firewall Configuration” on page 21

Server System Requirements

Reflection for Secure IT Gateway server components are supported on the following platforms:

- ◆ Windows Server 2019
- ◆ Windows Server 2016
- ◆ Windows Server 2012 R2 on Intel or equivalent, 64-bit
- ◆ Windows Server 2012 on Intel or equivalent, 64-bit
- ◆ VMWare vSphere Hypervisor (ESXi) running supported platforms

Gateway Administrator Web Application

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

- ◆ Microsoft Internet Explorer (version 11 or later, Windows only)
- ◆ Mozilla Firefox (current versions)
- ◆ Google Chrome (current versions)
- ◆ Apple Safari (current versions, Mac only)

PKI Services Manager

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

- ◆ Reflection PKI Services Manager version 1.3.2 or later

NOTE: For additional recommendations to help ensure a secure environment, see [“Security Recommendations for the Reflection Secure Shell Proxy” on page 130.](#)

Transfer Client Requirements

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

- ◆ Users must be running one of the following supported browsers. JavaScript and cookies must be enabled.
 - ◆ Microsoft Internet Explorer (version 11 or later, Windows only)

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

- ◆ Mozilla Firefox (version 52 ESR 32-bit)
- ◆ 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 [Java website \(http://www.java.com\)](http://www.java.com).

Connections from other Secure Shell Clients

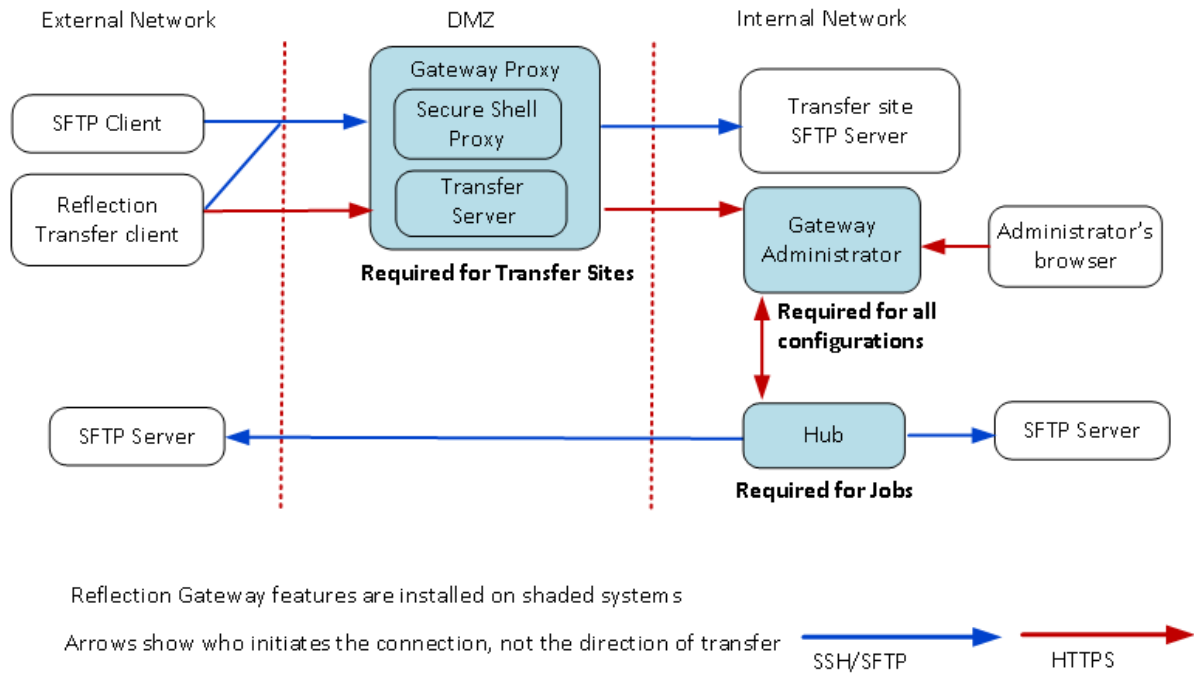
Using the Reflection Transfer Client to access Transfer Sites is not a requirement. Reflection Gateway users can also use the Reflection for Secure IT Secure Shell client, the Reflection FTP Client configured for SFTP transfer, or any other SFTP-enabled SSH client.

Reflection for Secure IT Gateway Components

In production environments, Reflection for Secure IT Gateway components are typically installed using a distributed configuration. The diagram below shows a sample configuration using all components required for both automated Jobs and Transfer Sites. See [Job Components \(page 10\)](#) and [Transfer Site Components \(page 12\)](#) for more information about each of these features.

- ◆ The Gateway Administrator service is required for all Reflection for Secure IT Gateway installations. It should be installed on a system in your internal network.
- ◆ The Reflection Transfer Server and Reflection Secure Shell Proxy are required for Transfer Sites. These two services must be installed together using the Setup Gateway Proxy feature. These services are typically installed on a system in the DMZ.
- ◆ The Reflection Hub is required for automated Jobs. This service should be installed on a system running in your internal network.
- ◆ The number and arrangement of SFTP servers depends on your business needs. These can be any UNIX or Windows servers running SFTP-enabled SSH. The diagram below shows one possible arrangement. Other variations might include:
 - ◆ Scan an internal SFTP server for files and trigger Job Actions that send these files to external servers available to your customers.
 - ◆ Designate an SFTP server as the Transfer Site file server and scan files for Job actions on this same server. With this arrangement you can configure automated Job Actions to act on files that are uploaded to by a Transfer Site user.
 - ◆ Use the Reflection Gateway Proxy as the Transfer Site file server.

NOTE: The Reflection for Secure IT Gateway installer includes the Reflection for Secure IT Server for Windows. Each Reflection Gateway license entitles you to install this SFTP-enabled server on one system. Contact Micro Focus for information about purchasing additional Reflection for Secure IT Servers for UNIX or Windows.



Related Topics

- ◆ [“Job Components” on page 10](#)
- ◆ [“Transfer Site Components” on page 12](#)
- ◆ [“Reflection for Secure IT Gateway Architecture” on page 15](#)

Installing Reflection Gateway

Before you install Reflection for Secure IT Gateway, review your configuration plan.

- ◆ For the simplest configuration, you can install all Reflection Gateway services on a single system. (The optional Reflection for Secure IT Server cannot be installed on this system.) This configuration can be useful for initial testing.
- ◆ For a distributed configuration, you will need to run the installer on each computer in your configuration. Review [Reflection for Secure IT Gateway Components \(page 18\)](#), [Job Components \(page 10\)](#), and [Transfer Site Components \(page 12\)](#) to determine which features you need to install on each computer.

NOTE: You must install the same version (and build) of all Reflection for Secure IT Gateway components.

To install Reflection Gateway

- 1 Log on to Windows using an Administrator account.

- 2 Start the Setup program. (When you download Reflection Gateway from the Micro Focus download site, you are first prompted to select a folder in which to extract the installation files. This is a temporary location. After this step is complete, the Setup program starts automatically.)
- 3 Reflection Gateway requires the Microsoft Visual C++ Redistributable Package. It is installed by the Setup program if it is not already on your system. If you see a message saying that this package must be installed, click **Continue** to install this required software. The Reflection Gateway installation continues after this prerequisite is installed.
- 4 Click the **Feature Selection** tab. All Reflection Gateway services are installed by default. This configuration is useful for evaluation and initial testing.

To create a distributed installation, deselect the features you don't want to install on each system. To do this, click the icon next to the feature name and select **Feature will be unavailable**. To add a feature, click the icon and select **Feature will be installed on local hard drive**.

Note the following:

- ◆ The **Reflection Gateway Proxy** feature always installs both the **Reflection Transfer Server** and the **Reflection Secure Shell Proxy**. These two services must always be installed together on the same server.
 - ◆ The **Reflection for Secure IT Server** cannot be installed on the same system as the **Reflection Secure Shell Proxy**.
- 5 (Optional) To change the default installation folder, click the **File Location** tab.
 - 6 Click **Install Now**.
 - 7 On the final installation screen, select **Restart my computer for me** and click **Close**.

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

To confirm that the installed services are running

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

- 1 Open the Windows Services console.
- 2 Confirm that the services are running. The following services are installed with Reflection Gateway features:

| Installed feature | Reflection Gateway service name |
|---|--|
| Reflection Gateway Proxy | Micro Focus Reflection Transfer Server |
| | Micro Focus Reflection Secure Shell Proxy |
| Reflection Gateway Administrator | Micro Focus Reflection Gateway Administrator |
| Reflection Hub | Micro Focus Reflection Hub |
| Reflection for Secure IT Server | Micro Focus Reflection for Secure IT Server |

(This feature is not included in a default installation. It cannot be installed on the same system as the Reflection Gateway Proxy feature.)

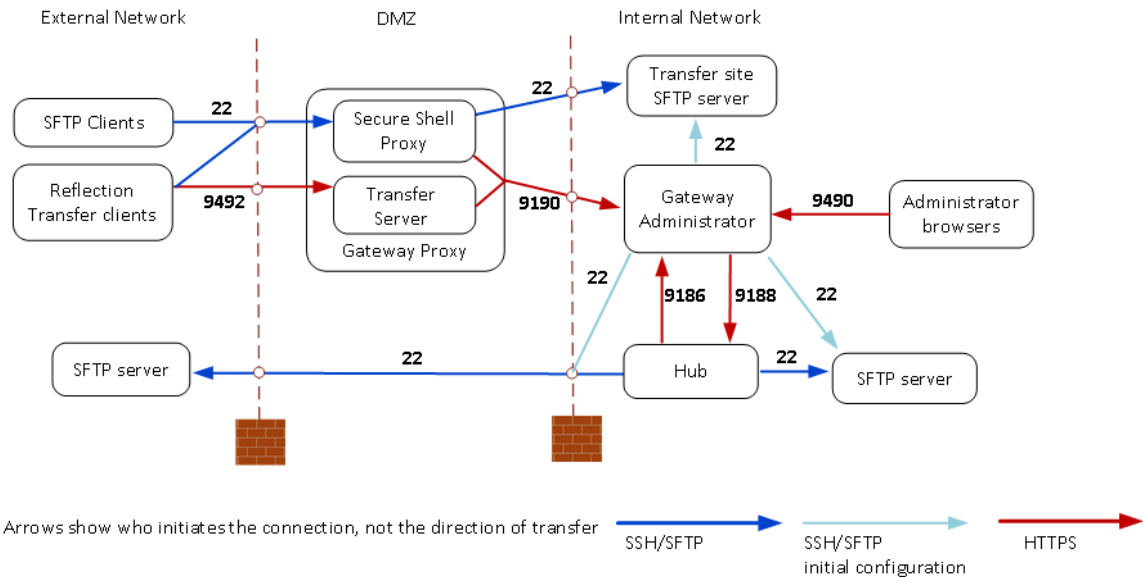
NOTE: After these services are started by a Windows system restart or by using the Services console, it might take a few minutes before they are available for use.

Related Topics

- “Ports and Firewall Configuration” on page 21
- “Start and Stop the Reflection Gateway Administrator Service” on page 140
- “Start and Stop the Reflection Transfer Server” on page 140

Ports and Firewall Configuration

Your firewall settings will depend on which Reflection Gateway features you use and how you have configured your installation. The diagram below shows which ports are used by default in a distributed configuration. The table that follows provides additional detail.



| Connection Description | Default Listening Port | Where to Change the Listening Port | Where to Specify the Port Used for the Connection |
|---|------------------------|--|---|
| Transfer clients to the Reflection Secure Shell Proxy | 22 | Reflection Secure Shell Proxy > Network pane | SFTP Client The value for the Reflection Transfer Client is set using Reflection Transfer Server container.properties > sftp.port. |
| Reflection Transfer Client to Reflection Transfer Server | 9492 | Reflection Transfer Server container.properties > servletengine.ssl.port | Reflection Transfer Client connection URL |
| Not used if you use an alternate SFTP client (page 63). | | | |

| Connection Description | Default Listening Port | Where to Change the Listening Port | Where to Specify the Port Used for the Connection |
|--|------------------------|--|---|
| <p>Reflection Secure Shell Proxy to Transfer Site SFTP server</p> <p>Not used if Transfer site file server (page 90) is set to Reflection Gateway Proxy (the default).</p> | 22 | SFTP server | New/Edit SFTP Server (page 91) |
| Reflection Transfer Server to Reflection Gateway Administrator web service | 9190 | Reflection Gateway Administrator container.properties > configservice-ws.port | Reflection Secure Shell Proxy > Reflection Gateway Users pane > Gateway Administrator port > Activate and verify |
| Administrative workstation browser to display Gateway Administrator user interface | 9490 | Reflection Gateway Administrator container.properties > servletengine.ssl.port | Gateway Administrator connection URL |
| Reflection Gateway Administrator to Reflection Hub | 9188 | Reflection Hub container.properties > hub.command-api.port | New/Edit Hub (page 93) |
| Reflection Hub to Reflection Gateway Administrator | 9186 | Reflection Gateway Administrator container.properties > configservice.response-api.port | New/Edit Hub (page 93) |
| Reflection Hub to SFTP servers | 22 | SFTP server | New/Edit SFTP Server (page 91) |
| <p>Gateway Administrator to SFTP servers</p> <p>The direct connection from Gateway Administrator to SFTP servers is not required for running Jobs or Transfer sites. Gateway Administrator makes this connection to retrieve the host key when you first add a server and to display server host directories in response to a Browse button.</p> | 22 | SFTP server | New/Edit SFTP Server (page 91) |
| <p>Browser launched by the Reflection Secure Shell Proxy to display the Gateway Administrator user interface.</p> <p>Not shown in diagram. This connection is only required if you want to launch the Gateway Administrator directly from the Reflection Secure Shell Proxy console.</p> | 9490 | Reflection Gateway Administrator container.properties > servletengine.ssl.port | No configuration is required; connection information is retrieved automatically using the Reflection Gateway Administrator web service. |

| Connection Description | Default Listening Port | Where to Change the Listening Port | Where to Specify the Port Used for the Connection |
|--|------------------------|------------------------------------|---|
| Reflection Gateway Administrator to Reflection PKI Services Manager | 18081 | PKI Services Manager | New/Edit PKI Server (page 96) |
| Not shown in diagram. This connection is used only if Authentication (page 94) is set to use X.509 certificates. | | | |

3 Initial Configuration

The procedures in this section describe the initial setup procedures that are required for using Reflection Gateway. These one-time procedures are performed by the Reflection Gateway administrator.

In this Chapter

- ♦ [“Initial Configuration Steps for Using Jobs” on page 25](#)
- ♦ [“Initial Configuration Steps for Using Transfer Sites” on page 25](#)
- ♦ [“How To...” on page 26](#)

Initial Configuration Steps for Using Jobs

This is an overview of initial configuration steps for using Jobs. Detailed procedures follow in the [How To](#) section. Steps do not need to be in this order. Steps 3 and 4 are required before Jobs can be added or run. Other steps are common to most implementations.

To configure Reflection Gateway for Jobs

- 1 [Log onto Gateway Administrator \(page 26\)](#).
- 2 [Configure email support \(page 30\)](#).
- 3 [Add one or more SFTP servers \(page 30\)](#).
- 4 [Add one or more hubs \(page 30\)](#).
- 5 [Configure access to directories on your SFTP servers \(page 29\)](#).
- 6 Configure access to Gateway Administrator for users who will manage Jobs. You can use either or both of these methods:
 - ♦ [Add users to the built-in ReflectionGateway user list \(page 35\)](#).
 - ♦ [Configure access to an external LDAP server \(page 37\)](#).
- 7 [Configure server certificates \(page 34\)](#).

If you are also going to use Transfer Sites, see [“Initial Configuration Steps for Using Transfer Sites” on page 25](#).

Related Topics

- ♦ [“Job Components” on page 10](#)
- ♦ [“How to Create and Test Jobs” on page 47](#)

Initial Configuration Steps for Using Transfer Sites

This is an overview of initial configuration steps for using Transfer Sites. Detailed procedures follow in the [How To](#) section. Steps do not need to be in this order. Step 1 is required before Transfer Sites can be used. Other steps are common to most implementations.

To configure Reflection Gateway for Transfer Sites

- 1 [Enable Reflection Gateway Connections in the Reflection Secure Shell Proxy \(page 32\)](#).
- 2 [Log onto Gateway Administrator \(page 26\)](#).
- 3 [Configure email support \(page 30\)](#).
- 4 [Set up the Transfer Site File Server \(page 33\)](#). (If you have added servers for Jobs, this can be one of those servers or it can be a different server.)
- 5 Provision users using either or both of these methods:
 - ♦ [Add users to the built-in ReflectionGateway user list \(page 35\)](#).
 - ♦ [Configure access to an external LDAP server \(page 37\)](#).
- 6 [Configure server certificates \(page 34\)](#).

If you are also going to use Jobs, see “[Initial Configuration Steps for Using Jobs](#)” on page 25.

Related Topics

- ♦ [“Transfer Site Components” on page 12](#)
- ♦ [“How to Create Transfer Sites and Transfer Files” on page 58](#)

How To...

- ♦ [“Log on to the Gateway Administrator” on page 26](#)
- ♦ [“Add File Servers to Gateway Administrator” on page 27](#)
- ♦ [“Set Up Directory Access on your SFTP Servers” on page 29](#)
- ♦ [“Add Hubs to Gateway Administrator” on page 30](#)
- ♦ [“Configure Email Support in Gateway Administrator” on page 30](#)
- ♦ [“Enable Reflection Gateway Connections in the Reflection Secure Shell Proxy” on page 32](#)
- ♦ [“Set Up the Transfer Site File Server” on page 33](#)
- ♦ [“Configure Server Certificates” on page 34](#)

Log on to the Gateway Administrator

Gateway Administrator is a web-based tool for provisioning users and configuring Jobs and Transfer Sites. Your initial log on resets the default administrative password.

Before you begin

[Install the Gateway Administrator \(page 19\)](#).

To connect to the Gateway Administrator and log on

- 1 You can connect using either of the following methods:

On the server running Gateway Administrator, use the Windows Start menu.

-or-

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

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

NOTE: You will see a warning message before you see the login page. This warning shows up because the Gateway Administrator installs with a self-signed security certificate that is unknown to your browser. For initial testing purposes, you can ignore this warning and proceed with the connection (Internet Explorer or Chrome) or add an exception (Firefox). For more information, see [“Server Certificate Management” on page 131](#).

2 For your initial log on, enter the following credentials:

Username: admin

Password: secret

3 Immediately after your first log on, you will be prompted to change the password for the admin account.

Use the next procedure to specify an actual email address for the default admin user. Use this procedure if you plan on doing initial testing of email notifications using this default user.

To update the email address of the default admin account

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

NOTE: It is not possible to reset a lost administrator account password. After you begin to provision actual users, you should add appropriate users to the Administrators group to replace the default admin account. This helps ensure that the correct users will have full access to Gateway Administrator configuration options, and that backup administrators are available to provide access if needed. For details about how to add Windows domain users to the Administrators group, see [“Add LDAP Users to the Administrators Group” on page 39](#).

Add File Servers to Gateway Administrator

SFTP file servers are used for both Jobs and Transfer Sites.

Jobs require at least one added file server. Job administrators can configure Reflection Gateway to scan for new and/or updated files on any added server. Jobs actions can then be used to transfer files to another location on the scanned server or to any other added server. Job actions can also be used to manage files by executing commands on any added server. If desired, the Gateway Administrator system administrator can set up [File Server Groups \(page 92\)](#) to limit which file servers Job administrators have access to when configuring Jobs.

Transfer Sites use a single designated Transfer Site file server for all transferred files. This server can be the default Gateway Administrator Proxy or any added server. Transfer Sites files are uploaded and downloaded to and from subdirectories created in the designated **Transfer site base directory**. For more information, see [“Set Up the Transfer Site File Server” on page 33](#).

NOTE: If you don't plan on configuring Jobs, and you use the default Gateway Administrator Proxy as your Transfer Site file server, you do not need to add additional file servers, so you can omit this procedure.

Before you begin

- ♦ Know the host name (or IP address) of the SFTP file server you want to add and the port used by this host for SFTP connections. (The standard port for SFTP connection is 22.) This can be any UNIX or Windows system running an SFTP-enabled SSH server.

NOTE: The Reflection for Secure IT Gateway installer includes the Reflection for Secure IT Server. Each Reflection Gateway license entitles you to install this SFTP-enabled server on one system. Contact Micro Focus for information about purchasing additional Windows or UNIX servers.

- ◆ Identify a user on this server whose User ID will be used for the connection to the server. To configure password authentication you will need to know the user's password. To configure public key authentication, public key authentication must be configured for the user on the server and you need access to the user's private key.

To add a File Server to Gateway Administrator

- 1 Log on to Gateway Administrator using the default admin account, or any account that has the **System setup** role enabled.
- 2 Go to **System > File Servers** and click **New**.
- 3 Enter the server name or IP address and the port used by this server for SFTP connections.
- 4 Click **Retrieve** to retrieve the host key.
- 5 For **UserID** enter the user whose credentials will be used to connect to this server.
- 6 Configure user authentication using one of the following:
 - ◆ Select **Password** and enter the user's password.
 - OR-
 - ◆ Select **Public key**. Click **Import key**, then browse to locate this user's private key. This imports the key into the Reflection Gateway database. After the import, you can delete the key from the file system to minimize security risks.
- 7 If you are configuring a server for Jobs, leave **Transfer site base directory** blank; this setting is not used for Job actions.

If you plan on using this server for your Transfer Site files, browse to select a **Transfer site base directory**. The directory you select must be available to the specified user account. The path you select is automatically entered using the correct syntax for your server. By default, the base directory is set to a subdirectory called `Reflection` in the directory you selected. This subdirectory is not required; you can edit or delete this subdirectory name.
- 8 Click **Test Connection**. (This tests the current on-screen settings. These settings are not saved until you click **Save**.)
- 9 Click **Save**.

Related Topics

- ◆ [“Set Up Directory Access on your SFTP Servers” on page 29](#)
- ◆ [“Create an Audit Log of File Transfers” on page 150](#)
- ◆ [“File Servers Tab” on page 90](#)
- ◆ [“File Server Groups Tab” on page 92](#)
- ◆ [“SFTP File Server Configuration Troubleshooting” on page 99](#)

Set Up Directory Access on your SFTP Servers

If you are going to use an SFTP server in Job actions, review this information to ensure that Job actions will have access to required directories on the server.

Each SFTP server you add to Gateway Administrator includes a **UserID** whose credentials provide access to this server. All transfers and commands executed on this server use the access rights of this user.

Job actions that transfer files use an SFTP connection running as the user specified for **UserID**.

- ◆ If you specify a relative path for a transfer destination, files are transferred to a location relative to the SFTP home directory of this user.
- ◆ If you specify an absolute path for a transfer destination, the location must be accessible to this user from an SFTP session.

Job actions that execute commands run a remote SSH command as the user specified for **UserID**. The action runs in a shell session from the user's home directory.

- ◆ Commands specified without path information run in the SSH home directory of the user.
- ◆ If you specify a relative path for command output, files are created in a location relative to the home directory of user.
- ◆ If you specify an absolute path for command output, the location must be accessible to the user in an SSH terminal session.

If you want files to land in a location other than the user's home directory, you need to configure your SFTP server to provide access to the required directories. The approach you use depends on your server type.

Configuring Directory Access on a Reflection for Secure IT Server for Windows

On a Reflection for Secure IT Server for Windows, the SSH terminal directory is configured on the **Permissions** pane. The default is the user's Windows Profile directory. When configuring fully qualified paths for Job actions that execute commands, use the actual Windows path (for example `c:\Users\Joe`).

The Reflection for Secure IT Server provides SFTP directory access using virtual directories. By default users log into a virtual directory called `Home`, which is mapped to the user's Windows Profile directory. When configuring fully qualified paths for Job actions that transfer files, use the virtual directory name (for example `\Home`). If you want to configure Job actions that transfer files to a different location, you can configure additional virtual directories. The following procedure shows how to create a virtual directory called `destination` that is mapped to the physical location `c:\destination` on the server.

To configure an additional accessible directory on a Reflection for Secure IT Server for Windows

- 1 Start the Reflection for Secure IT Server for Windows console and open the **Configuration** tab.
- 2 Click **SFTP Directories** and click **Add**.
- 3 For **Virtual directory** specify the directory name you want to use in Job actions that transfer files (for example `destination`).
- 4 For **Local or UNC directory** enter the actual path to a directory available to **UserID** on this server (for example `c:\destination`).
- 5 Click **OK**.
- 6 Save your settings (**File > Save Settings**).

Configuring Directory Access on a UNIX Server

On UNIX servers, both the default SSH and SFTP home directories are typically the same (for example `/home/joe`).

If you want to configure Job actions that transfer files or create files in a different location, you can use UNIX system commands to specify a different home directory for the user.

Add Hubs to Gateway Administrator

Hubs are required to support Reflection Gateway Jobs. You must add at least one Hub before you can configure Jobs.

Hubs are not used for Transfer Sites; if you use only Transfer Sites, you can skip this procedure.

Before you begin

- ◆ [Install the Reflection Hub feature on the Hub server \(page 19\)](#).

You will need to know a host name or IP address that can be used by Gateway Administrator to connect to this Hub.

To add a Hub Server to Gateway Administrator

- 1 Log on to Gateway Administrator using the default admin account, or any account that has the **System setup** role enabled.
- 2 Go to **System > Hubs** and click **New**.
- 3 For **Reflection Hub server**, enter the name or IP address of the Reflection Hub. The correct default listening port is entered automatically. Unless an administrator has modified this port, do not edit this value.

The name and currently configured listening port for the server running the Reflection Gateway Administrator service are entered automatically. In most cases you should leave these as entered.

- 4 Click **Save and Activate**. This tests the connections between the servers and configures certificates that are used by each server for authentication in subsequent connections. (For details, see [“Hubs Tab” on page 93](#).)

NOTE: You can add multiple Hubs to ensure availability of the Reflection Hub service. If you configure connections to more than one Hub, Reflection Gateway uses a round robin schedule to determine which Hub to connect to.

Related Topics

- ◆ [“Hubs Tab” on page 93](#)
- ◆ [“Managing Jobs” on page 47](#)
- ◆ [“Hub Configuration Troubleshooting” on page 99](#)

Configure Email Support in Gateway Administrator

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

- ◆ Account creation email for new users
- ◆ Job success and failure notifications

- ◆ Password reset email
- ◆ Transfer site access notifications
- ◆ Notifications sent to Transfer Site managers and/or Transfer Site members when files are uploaded or downloaded

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

To configure the email server connection

- 1 Log on to Gateway Administrator using the default admin account (or any account that has the **System setup** role enabled).
- 2 Go to **System > Email Server**.
 - ◆ Set **Email service** to **Enabled**. This step is required to make the remaining items editable.
 - ◆ For **SMTP server**, enter your email server name or IP address.
 - ◆ Configure additional options appropriate for your mail server. For details, see [“Email Server Tab” on page 88](#).
 - ◆ If **Check server identity** is selected (recommended), click **Retrieve Certificate**.
- 3 Click **Test Connection**. (This tests the current on-screen settings. These settings are not saved until you click **Save**.)
- 4 Click **Save**.

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

To test an outgoing message using your email server settings

- 1 Click the **Email Templates** tab. The Account Creation template is displayed by default.
- 2 Below the template text, click **Preview** to expand this portion of the page.
- 3 Enter your email address in the **To** box.
- 4 Click **Send Test Email**. You should receive a sample Account Creation email.

Configuring the URL for Transfer Site Email Messages

Some emails sent from Gateway Administrator include a URL that Reflection Gateway users can use to set a password or connect to the Reflection Transfer Client. By default, these links use "localhost" as the server address. If you are creating and configuring Transfer Sites that use these emails, you need to configure Gateway Administrator to create links that connect correctly to the actual Transfer Server address. To do this, you edit the [Gateway Administrator Properties File \(page 117\)](#), as described in the next procedure.

To configure the base server URL used in Transfer Site email message links

- 1 As an administrator of the system running Gateway Administrator, open the Gateway Administrator `container.properties` in a text editor. The default location of this file is:


```
C:\Program Files\Micro
Focus\ReflectionGateway\GatewayAdministrator\conf\container.properties
```
- 2 Locate the following lines:

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

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

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

- 4 Save the edited properties file.
- 5 [Restart the Micro Focus Reflection Gateway Administrator service \(page 140\)](#). A restart is required after any changes to the properties file.

Related Topics

- ◆ [“Email Administration” on page 111](#)
- ◆ [“Email Troubleshooting” on page 107](#)

Enable Reflection Gateway Connections in the Reflection Secure Shell Proxy

This procedure applies to Transfer Sites only. It is not required for creating and using Jobs.

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

Before you begin

- ◆ Install the Reflection Gateway Proxy services and the Gateway Administrator.

To enable Reflection Gateway Transfer Site transfers

- 1 Log in as an administrator to the Windows system on which you installed the Reflection Gateway Proxy. Use the Windows Start menu to launch the Reflection Secure Shell Proxy console.
- 2 On the **Reflection Gateway Users** pane, enable **Allow access to Reflection Gateway users**.
- 3 For **Gateway Administrator host**, enter the name or IP address of the computer running the Reflection Gateway Administrator. (If you installed all Reflection Gateway services on the same computer, you can leave the default value, `localhost`.) Leave the default port value (9190). Reflection Gateway Administrator is configured to listen on this port by default.
- 4 (Optional) change the value for **Reflection Gateway user access account** from the default (**Service account**) to an actual **User account** on the system. The following factors may enter into this decision:
 - ◆ When **Service account** is selected, Reflection Gateway users run using the same privileges as the Reflection Secure Shell Proxy service (the Local System account). You may want to specify an alternate user account with more limited privileges.
 - ◆ Running as the service account is limited by the operating system to 110 simultaneous client connections. Configuring a **User account** does not have this limitation.
- 5 Click **Activate and verify**. This saves your settings and triggers actions that ensure that the Reflection Gateway Proxy services can establish a secure connection with the Gateway Administrator.
 - ◆ You will be prompted to accept the certificate presented by the Gateway Administrator server. Click **Yes** to establish the trust relationship.

- When the configuration update is complete, click **Close** to close the **Web service connection** dialog box.
- Click **Yes** when prompted to restart the Reflection Transfer Server service. This step is required.

Set Up the Transfer Site File Server

This procedure applies to Transfer Sites only. It is not required for creating and using Jobs.

Reflection Gateway Transfer Sites use directories on a designated Transfer Site file server for file upload and download. Use the procedures described here to designate which server should be used.

Use the Reflection Gateway Proxy for Transfer Site files

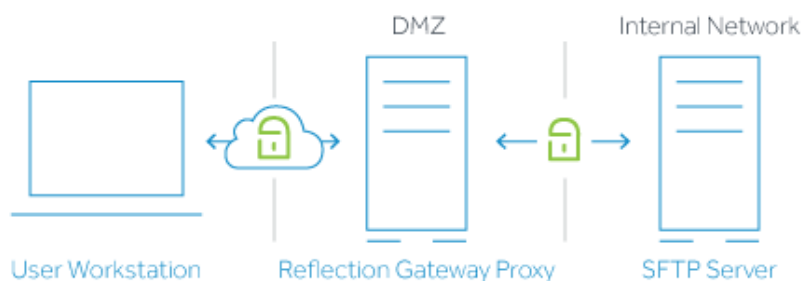
By default, Gateway Administrator is configured to use the Reflection Gateway Proxy for as the Transfer Site file server. Files are transferred to and from this server. This configuration is appropriate for initial testing, or if you use Transfer Sites to manage transfers within your internal network. You do not need to modify any default settings to use this configuration.



To customize the base directory used for files on the Reflection Secure Shell Proxy, see [“Change the Transfer Site Directory used by the Reflection Secure Shell Proxy”](#) on page 127.

Use an added SFTP server for Transfer Site files

Transferring files to and from an added SFTP server is recommended for most environments. If you run the Reflection Gateway Proxy in the DMZ, you can configure Reflection Gateway to transfer files securely to and from an SFTP server running behind your firewall. In this configuration, data streams continuously through the Reflection Secure Shell Proxy, eliminating the need to save data on the system running the proxy.



An additional advantage of this configuration is that it supports [Post Transfer Actions](#) (page 64). These actions are not supported when the Reflection Gateway Proxy is the Transfer Site file server.

To set up the added SFTP server

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

- 2 [Add the SFTP server to the list of available servers \(page 27\)](#).
- 3 In the **New** (or **Edit**) **File Server** page, set **Transfer site base directory** to the directory you want to use for Transfer Site file exchange.

NOTE: If you use the Browse button to specify a directory on the server, Gateway Administrator automatically adds a `Reflection` subdirectory to the path to help ensure that Transfer Site files are easy to locate on the server. This subdirectory is not required; you can edit the path to modify or remove the subdirectory name if you prefer.

- 4 Click **Save**.
- 5 In the **File Servers** tab, use the **Transfer site file server** drop-down list to select the added SFTP server.
- 6 Click **Save**.

Configure Server Certificates

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

Why you see certificate warning messages

When an HTTPS connection is established, the browser requires server authentication. By default, the Reflection Gateway servers send a self-signed security certificate to the browser for this purpose. (A self-signed certificate is signed by the same entity that it certifies.) The browser checks the digital signature in this certificate against its list of trusted [Certificate Authorities \(CAs\) \(page 153\)](#). 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 Reflection Gateway evaluation and configuration process, you can use any of the following approaches to manage server certificates.

- ♦ Use the default self-signed certificates and ignore the certificate errors.

This option is appropriate during initial testing.

- ♦ [Configure your browser to trust the self-signed certificates \(page 134\)](#).

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

- ♦ [Replace the server's self-signed certificate with a certificate from a well-known Certificate Authority \(page 131\)](#).

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

4 Managing Users and Groups

- ◆ “Add Users to the Default User List” on page 35
- ◆ “Delete or Disable Users” on page 36
- ◆ “Provision Users from an Added LDAP Server” on page 37
- ◆ “Add LDAP Users to the Administrators Group” on page 39
- ◆ “LDAP Server Advanced Domain Settings” on page 40
- ◆ “Creating and Editing Groups” on page 42
- ◆ “Roles in Reflection Gateway” on page 43
- ◆ “Configure Certificate User Authentication” on page 44
- ◆ “Set Up PKI Services Manager” on page 45

Add Users to the Default User List

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

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

| Method | Features |
|--------------------------------------|---|
| Users > New | <ul style="list-style-type: none">◆ Add users as a separate step for use with either Jobs or Transfer Sites.◆ Configure both UserID and Email address. These can be the same or different.◆ Choose either Email registration or Specify password. If you select Specify password, no email is sent automatically from Reflection Gateway; you must send login credentials to the user in a secure way.◆ Configure group membership when you add the user. NOTE: If you are using email registration, do not configure group membership in any group with access to Gateway Administrator. Email registration is not available to these users.◆ Required Role: Manage Reflection Gateway users. |
| Transfer Sites > Quick Add | <ul style="list-style-type: none">◆ Add a user when a new Transfer Site is created.◆ UserID is set automatically to the user's email address.◆ User is added with no group membership. Users can be added to groups later.◆ User is given default site permissions. Site permissions can be modified later by editing the Transfer Site.◆ Required Roles: Manage Reflection Gateway users and Manage transfer sites. |

| Method | Features |
|---|--|
| Transfer Sites > Add (or Edit) | <ul style="list-style-type: none"> ◆ Add a user when you create a new Transfer Site or edit an existing site. ◆ UserID is set automatically to the user's email address. ◆ User is added with no group membership. Users can be added to groups later. ◆ Modify the default site permissions for any user (new or existing). ◆ Required Roles: Manage Reflection Gateway users and Manage transfer sites. |

To add a user from the New User page

- 1 Connect to Gateway Administrator and log in using an account that is a member of the Administrators Group, the File Transfer Administrators group, or any group that has the **Manage Reflection Gateway users** role enabled.
- 2 On the **Users** tab, click **New**.
- 3 Enter user information. See [“New User” on page 81](#) for details. Note the following:
 - ◆ To support **Email registration**, [email support must be configured \(page 111\)](#).
 - ◆ If you select **Specify password**, no email is sent automatically from Reflection Gateway; you must send login credentials to the user in a secure way.
 - ◆ Group membership is optional. All Reflection Gateway users can log on to the Reflection Transfer Client, and Transfer Site access can be configured for individual users or groups.
 - ◆ Do not configure group membership if you are using email registration. Email registration is not available to users in any group that has access to Gateway Administrator.
- 4 Click **Save**.

Related Topics

- ◆ [“Use Quick Add to Add Transfer Sites and Users” on page 62](#)
- ◆ [“Create a Transfer Site” on page 58](#)
- ◆ [“Managing Users and Groups” on page 35](#)

Delete or Disable Users

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

NOTE: LDAP user accounts must be managed on the LDAP server.

To delete a Reflection Gateway user

- 1 Connect to Gateway Administrator and log in using an account that is a member of the Administrators Group, the File Transfer Administrators group, or any group that has the **Manage Reflection Gateway users** role enabled.
- 2 On the **Users** tab, select the user and click **Delete**. You will be prompted to confirm this action.

To disable a Reflection Gateway user

- 1 Connect to Gateway Administrator and log in using an account that is a member of the Administrators Group, the File Transfer Administrators group, or any group that has the **Manage Reflection Gateway users** role enabled.
- 2 On the **Users** tab, select the user and click **Edit**.
- 3 Set **Account expires** to a date in the past. (To enable an expired account, set this to a date in the future.)

Provision Users from an Added LDAP Server

Use the **LDAP Servers** tab to add users to Reflection Gateway who have accounts in Windows Active Directory. You can use this approach to provide Transfer Site and Gateway Administrator access to Windows domain users. Authentication is managed on the LDAP server. Each time the user logs in, current information is retrieved from the LDAP server.

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

To add access to users in an LDAP server

- 1 Log on to Gateway Administrator using an account in the Administrators group (or any account that has the **System setup** role enabled).
- 2 Go to **System > LDAP Servers**.
- 3 Click **New**.
- 4 Enter information for connecting to your LDAP server. For details, see [“New/Edit LDAP Servers Tab” on page 86](#).

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

```
mydomain\user
```

-or-

```
user@mydomain
```

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

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

To view LDAP users and groups

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

NOTE: After you have added an LDAP server, you should [add one or more users from this server to the Gateway Administrator Administrators group](#). Gateway Administrator does not support password reset for users who have access to Gateway Administrator. Adding administrators from an added

LDAP server ensures that backup administrators are available to provide access if needed because these users will have full access to Reflection Gateway configuration using their Active Directory log on credentials.

Customizing the domain\username login format accepted for users in an added LDAP server

Users who have been added to the built-in ReflectionGateway list can log into the Transfer Client and/or Gateway Administrator using just a user ID (for example `joe`) or using the domain name and user ID (`ReflectionGateway\joe`).

When users log in using an account in an added LDAP server, authentication is handled by the LDAP server. The login requirements in this case depend on the LDAP server requirements and how you have configured the added LDAP server in Gateway Administrator. You can use **Advanced domain settings** on the **New/Edit LDAP Server (page 86)** page to customize how Reflection Gateway sends user credentials to the LDAP server. For example, you can use **Advanced domain settings** to specify a default domain name so that users do not need to include the domain name when they log in even if this is required by the LDAP server.

NOTE

- ◆ Reflection Gateway searches all available LDAP servers for a matching user and authenticates the first matching user it finds; it does not search additional LDAP servers if that fails.
 - ◆ When no domain name is included, a UserID for a different domain could match and allow login if the passwords for both accounts are the same.
 - ◆ **Advanced domain settings** apply to password authentication only; X.509 certificate authentication always requires user mapping that specifies both a domain and username.
-

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

Example 1

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

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

Example 2

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

- ◆ Login as `validUser`: Authentication succeeds because Reflection Gateway adds the value specified for Default Authentication Domain (`acme`) before authenticating the user.

- ◆ Login as `anyName\validUser` or `anyAlias\validUser`: Authentication fails because `anyName` and `anyAlias` are not valid authentication domain names.
- ◆ Login as `acme\validUser` or `acme.com\validUser`: Authentication succeeds because `acme` and `acme.com` are valid authentication domain names.

Example 3

Domain Name = `anyName`; Domain Mapping = `anyAlias`; Remove User Domain= **Yes**, Default Authentication Domain = none.

The following results are based on the sample `acme` domain, which requires a valid domain name for authentication:

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

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

Example 4

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

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

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

Add LDAP Users to the Administrators Group

After you have added an LDAP server, you should add one or more users from this server to the Gateway Administrator Administrators group. Gateway Administrator does not support password reset for users in the ReflectionGateway LDAP server. Adding administrators from an added LDAP server ensures that backup administrators are available to provide access if needed because these users will have full access to Reflection Gateway configuration using their Active Directory log on credentials.

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

To add LDAP users to the Administrators group

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

LDAP Server Advanced Domain Settings

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

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

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

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

Example 1

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

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

Example 2

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

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

Example 3

Domain Name = `anyName`; Domain Mapping = `anyAlias`; Remove User Domain= **Yes**, Default Authentication Domain = `none`.

The following results are based on the sample `acme` domain, which requires a valid domain name for authentication:

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

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

Example 4

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

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

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

Creating and Editing Groups

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

There are two ways to change ReflectionGateway group membership.

- ◆ Edit a group

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

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

Required role: **System setup**

- ◆ Edit a user

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

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

Required roles: **System setup** and **Manage Reflection Gateway users**

To add a new group

- 1 On the **Groups** page, set **LDAP Server** to ReflectionGateway.
- 2 Click **New**.
- 3 Enter a **GroupID** and **Description**.
- 4 (Optional) Assign [roles \(page 43\)](#) to this group.
- 5 Click **Save**.

To edit a group's list of members

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

NOTE: Clicking **Add** saves the change to the group.

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

To edit a user's group membership

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

Default Groups

Reflection Gateway includes two default groups.

- ♦ The Administrators group enables members to perform all available actions. The roles in this group cannot be modified and you cannot delete this group.
- ♦ The File Transfer Administrators group enables members to manage users, jobs, and Transfer Sites. The roles in this group cannot be modified and you cannot delete this group.

Roles in Reflection Gateway

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

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

The following roles are available:

| Role | Permissions |
|--|---|
| System Setup | Can view Groups , System , and About . Can modify all system settings. Can add groups and edit groups and modify the membership list of a group. |
| Manage actions | Can view Actions and About . Can create and edit Post Transfer Actions. |
| Manage transfer sites | Can view Transfer Sites and About . Can create and edit Transfer Sites. Can add existing users and groups to sites. Can add new sites using Quick Add , but cannot provision new users this way unless Manage Reflection Gateway users is also enabled. Cannot view the New Reflection Gateway User section of the New Transfer Site page unless Manage Reflection Gateway users is also enabled. |
| Manage jobs | Can view Jobs and About . Can create and edit Jobs. |
| Manage Reflection Gateway users | Can view Users and About . Can add and edit Reflection Gateway users and passwords. Cannot modify group membership. |

Related Topics

- ♦ [“Creating and Editing Groups” on page 42](#)

Configure Certificate User Authentication

By default, Transfer Site user authentication is done using a user name and password. You can also configure authentication using X.509 certificates, for example using a smart card.

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” on page 45](#).

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

- ◆ You must know the host name or IP address of the PKI server, and the listening port used by this server (18081 is the default).

Configure Gateway Administrator to contact your PKI Services Manager

- 1 Log on to Gateway Administrator using an account in the Administrators group (or any account that has the **System setup** role enabled).
- 2 On the **System** tab, click **PKI Servers**.
- 3 Click **New**.
- 4 For **PKI Server**, specify the name or IP address of the system running [PKI Services Manager \(page 45\)](#).
- 5 Click **Retrieve Public Key**.

If the server is running and available, Gateway Administrator retrieves the public key and displays it. (This key should match the key displayed in the PKI Services Manager console when you go to **Utility > View Public Key**.)

- 6 Click **Test Connection**. If Gateway Administrator can successfully contact PKI Services Manager, you will see a message saying the connection is successful.
- 7 Click **Save**. This step is required; verifying the connection does not save the configuration. You will be returned to the PKI Servers tab with your added server visible in the list.

Enable Certificate authentication for Transfer Client users

This procedure is required if users will connect using the Reflection Transfer Client.

- 1 From the Gateway Administrator **System** tab, click **Authentication**.
- 2 Select **Client X.509 certificate authentication**.
- 3 Click **Save**.

NOTE: When Client X.509 certificate authentication is selected, certificate authentication is required for all Reflection Transfer Client users. This setting does not affect connections from alternate clients.

Configure the SFTP client system

After you have completed the procedures above, subsequent user logins will not display a user name and password prompt. Login will succeed only if the SFTP client you are using is configured to present user certificates.

- ◆ If users connect using the Reflection Transfer Client, the browser needs to be configured to present the user certificate. For example, you might have users connect from a laptop with a built-in smart card reader that adds smart card certificates to the browser or system certificate store. Other options include installing a PKCS#11 client, such as ActivClient, onto user systems or importing user certificates manually into the browser or system certificate store.
- ◆ If users connect from an alternate SFTP client, the alternate client needs to be configured for certificate authentication. For example, in the Reflection for Secure IT Client for Windows, you can configure certificate authentication for SFTP connections using the Reflection Certificate Manager and the Secure Shell Settings dialog box.

If a user certificate is available on the client system, Gateway Administrator sends the certificate to PKI Services Manager for validation. If the certificate is valid, PKI Services Manager uses the preconfigured identity mapping to return the name of the user who is authorized to authenticate with the presented certificate.

Related Topics

- ◆ [“Certificate Authentication Fails” on page 105](#)
- ◆ [“Authentication Tab” on page 94](#)

Set Up PKI Services Manager

Reflection PKI Services Manager is a service that provides certificate validation services. If your client users will authenticate using smart cards or other forms of X.509 certificates, you need to install and configure this service. It is available at no additional charge from the Reflection Gateway download page. Reflection Gateway requires version 1.3.2 or later.

If you installed PKI Services Manager on Windows, you can configure required settings using the PKI Services Manager Console. 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> (<http://support.attachmate.com/manuals/pki.html>).

PKI Services Manager Configuration

- 1 Download and install PKI Services Manager.
PKI Services Manager can run on both Windows and UNIX systems. You can install it on the same system as Gateway Administrator or on another system in your network.
- 2 Create a certificate store that contains the CA certificates that are required to validate your user certificates. On Windows, you can create a private certificate store or use the Windows certificate store. On UNIX, you need to create a private store (or use an existing store on your system).
- 3 Specify one or more certificates to act as trust anchors; and specify where PKI Services Manager should search for intermediate certificates when building a path to your trust anchors.
In the console, use the **Trusted Chain** pane. Or, in `pki_config`, use the **TrustAnchor** and **CertSearchOrder** keywords.
- 4 Configure how PKI Services Manager should handle certificate revocation checking.

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

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

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

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

- 6 Save all settings changes and restart the PKI Services Manager server.

Sample Mapping Rules for Transfer Client Authentication

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

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

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

```
{ %Subject.CN% }      The allowed user name is equal to the value of the Subject Common Name field.
{ acme\%UPN.User% }  The allowed user name is constructed by combining the domain acme\ with the
                    value found in the userID portion of the UPN field.
```

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

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

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

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

5 Managing Jobs

Use Jobs to monitor the content of a directory and initiate Job actions automatically when new files are added to the scanned directory or existing files are updated. This flexible feature enables you to:

- ♦ Monitor directories on any added SFTP file server.
- ♦ Create a customized, ordered sequence of Job actions to handle new and updated files. Actions can include:
 - ♦ Moving or copying files to any added server.
 - ♦ Executing any command supported on the server where files first arrive, or on subsequent servers to which files are moved. For example, you can use system commands to delete or rename files, or run a command-line executable such as a virus scanner.

If any action in your sequence fails, no further actions take place. This ensures that the processes you configure to secure your site are successfully completed on all files.

- ♦ Configure email notification to alert system administrators when Job actions fail or succeed.
- ♦ Specify which directory to scan and whether or not to include subdirectories.
- ♦ Define the window of time that the directory will be monitored. For example, Monday through Friday from 8 AM to 5 PM.
- ♦ Set the scan interval to determine how frequently scans occur, for example every 30 minutes.
- ♦ Specify which files in the directory should be acted on, for example all PDF files, or all files of a given size.
- ♦ Specify the minimum number of files that must arrive before Job actions begin.
- ♦ Set up File Server Groups to enable users to configure Jobs only on specific file servers.

In this Chapter

- ♦ [“How to Create and Test Jobs” on page 47](#)
- ♦ [“Job Tokens” on page 55](#)

How to Create and Test Jobs

The procedures in this section are geared to users who are members of the default File Transfer Administrators group, or other groups with the **Manage jobs** role enabled. These procedures assume that [initial configuration \(page 25\)](#) has already been completed by a Reflection Gateway administrator.

In this Section

- ♦ [“Connect to Gateway Administrator” on page 48](#)
- ♦ [“Create a Job” on page 48](#)
- ♦ [“Configure a Job Action that Transfers Files” on page 50](#)
- ♦ [“Configure a Job Action that Executes a Command” on page 52](#)
- ♦ [“Notes for Testing Job Actions” on page 54](#)

Connect to Gateway Administrator

Gateway Administrator is a web-based application that you can use to manage users and Jobs.

Before you begin

- ◆ Know the address of the server running Reflection Gateway Administrator
- ◆ Have login credentials for an account that is a member of the File Transfer Administrators group, the Administrators group, or any group with the **Manage jobs** role enabled.

To connect to Gateway Administrator

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

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

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

Create a Job

To create a Job, you designate a server and directory to scan, set a scan interval, and optionally set filters to determine which files in the directory should trigger the actions you define in the **Actions** list. When Reflection Gateway detects new or updated files in the scanned directory that meet the filter conditions, it executes your defined Job actions.

Note that you can configure one or more actions for each Job. Reflection Gateway executes actions in the order listed. If an action fails:

- ◆ If a **Failure** email is configured, the email is sent to specified recipients.
- ◆ No subsequent actions are processed.

Before you begin

- ◆ To create a Job, you must be a member of the File Transfer Administrators group, the Administrators group, or any group with the **Manage jobs** role enabled.
- ◆ Initial configuration of SFTP servers, Hubs, and email should be complete. This must be done by a user with **System setup** privileges.

To create a new Job

- 1 [Log in to Gateway Administrator \(page 48\)](#).
- 2 Go to **Jobs > New**.
- 3 For **Name**, enter a descriptive name for the Job.
- 4 Leave **Disabled** selected for initial testing. You can use the **Run Now** feature to test disabled Jobs. After you are satisfied that the Job runs as expected, select **Enabled** to run the Job at the specified scan interval.
- 5 Under **Source Files**, configure the following:

| | |
|----------------------|---|
| Server | Select the server you want to scan. |
| Directory | Browse to select the server on the directory to scan for new or updated files. |
| Recursive | (Optional) Select Recursive if you want the scan to include subdirectories of the specified directory. |
| Scan Interval | (Optional) By default the directory is scanned every 10 minutes. You can change the frequency or days for scanning. |
| Filters | (Optional) By default all files are scanned. You can filter by name, size, modified time. You can also configure a minimum number of files that must arrive before Job actions begin. Use the check box to invoke the Failure email notification if no files meet the filter conditions at the end of the scan interval. |

6 Under **Actions**, from the **Add action...** drop-down list, select either **Transfer file** or **Execute command**. For details see:

- ◆ [“Configure a Job Action that Transfers Files” on page 50](#)
- ◆ [“Configure a Job Action that Executes a Command” on page 52](#)

7 (Optional) Under **Success** and **Failure**, click **Change** to configure email notifications.

8 Click **Save**.

9 Click **Run Now** to test. You’ll see a Running Job message. You can close this message at any time; it has no effect on execution of Job actions.

NOTE: If you make modifications to your Job, ensure that there are new or updated files in the scanned directory before each test.

10 (Optional) Configure additional actions for this Job.

11 After your **Run Now** tests work as expected, click **Enabled** and save the Job to have the Job run automatically on the specified **Scan Interval**.

To copy an existing Job

You can copy existing Jobs to create new Jobs based on existing Jobs.

1 On the **Jobs** tab, select the Job you want to copy and click **Copy**. A renamed copy of the selected Job is added to your Jobs list.

NOTE: All copied Jobs are marked as **Disabled** initially. This ensures that you don’t have identical Jobs running simultaneously.

2 Edit the copied Job and test it using **Run Now**.

3 After your **Run Now** tests work as expected, click **Enabled** and save the Job to have the Job run automatically on the specified **Scan Interval**.

Related Topics

- ◆ [“Notes for Testing Job Actions” on page 54](#)
- ◆ [“Job Troubleshooting” on page 100](#)

Configure a Job Action that Transfers Files

Use this procedure to configure automated file transfer between servers. The source server can be the scanned server or a server that received files from a previous action. The destination can be a different server or a different directory on the same server.

To configure a Job action that transfers files

- 1 [Create a Job and specify the scan server and directory.](#)
- 2 On the **New Job** (or **Edit Job**) page, under **Actions**, from the **Add action...** list, select **Transfer file**.
This opens the **Transfer File** dialog box.
- 3 (Optional) Select **Move** if you want to delete files from the source location after the transfer.
- 4 (Optional) Select **Preserve file attributes** if you want the modification date and time on the destination server to match the source. When this option is not selected, the destination file's timestamp shows the date and time of the transfer.
- 5 Configure the source server:
 - ◆ For **From**, select the source server from the list of available servers. If this is the initial transfer, select the scanned server.
 - ◆ Enter an expression to describe the files to transfer. For most transfers, use `$(SCANNED_PATH)/$(RELATIVE_FILE_NAME)` (the default) for the initial transfer. This will transfer all updated files on the scanned server that meet your filter criteria. If the scan is recursive, this option will also include all subdirectories in that directory. For subsequent transfers, replace `$(SCANNED_PATH)` with the correct actual path for the files on the server you are transferring from.
- 6 Configure the destination server:
 - ◆ For **To**, select the destination server.

NOTE: If [File Server groups \(page 92\)](#) have been configured by a Reflection Gateway administrator, the list of servers available to you is determined by your membership in one or more File Server groups.

 - ◆ Enter an expression to identify the location and naming pattern you want to use for files on the destination server. The expression you enter for destination files can use a combination of text and [tokens](#). For details, see [Entering Expressions for Destination Files](#) below.
- 7 Click **OK** to close the **Transfer File** dialog box.
- 8 Click **Save**.
- 9 Click **Run Now** to test the transfer. (If this is a repeat test, first update the files in the source location.)

Entering Expressions for Destination Files

The expression you enter for destination files in the Transfer File dialog box can use a combination of text and tokens. Refer to the examples below to understand how Reflection Gateway interprets these expressions. Note the following:

- ◆ **UserID** in these descriptions is the user whose **UserID** is configured for authentication to the destination SFTP server. (See [“New/Edit SFTP Server” on page 91.](#)) Any destination location you specify must be accessible to this user.

- ◆ If the destination server is a Reflection for Secure IT Server for Windows, specify destination paths using the virtual directory names that have been made accessible to **UserID**, not the actual physical directories on the server. (Virtual directory access is configured using the console's **SFTP Directories** pane.)
- ◆ If the destination server is a Reflection for Secure IT Server for UNIX (or other UNIX server), specify actual physical paths; UNIX servers do not use virtual directories.
- ◆ Use forward slashes (/) for specifying paths on both Windows and UNIX servers.

| Destination Expression | Output on Destination Server |
|--------------------------------------|--|
| \$RELATIVE_FILE_NAME\$ (the default) | <p>Files are created in UserID's SFTP login directory. The token is replaced by the relative path and filename of each file on the scanned server.</p> <p>If the scan is recursive, subdirectories that don't yet exist are created in the login directory.</p> <p>If the scan is not recursive, files in subdirectories are not transferred, and this token is equivalent to \$FILENAME\$.</p> |
| \$FILENAME\$ | <p>Files are created in UserID's SFTP login directory. The token is replaced by the filename of each file on the scanned server.</p> <p>If the scan is recursive, files are not transferred to subdirectories. All files—including those in subdirectories on the scanned server—are transferred to the SFTP login directory.</p> |
| upload/\$RELATIVE_FILE_NAME\$ | <p>Files are created in a subdirectory called <code>upload</code> in UserID's SFTP login directory. If this directory does not exist, it is created.</p> <p>If the scan is recursive, subdirectories are created in the <code>upload</code> directory.</p> |
| /upload/\$RELATIVE_FILE_NAME\$ | <p>Files are created in a directory called <code>upload</code> in the root directory. UserID must have write access to this directory.</p> <p>In most cases, the <code>upload</code> directory must already exist:</p> <ul style="list-style-type: none"> ◆ If the server is a Reflection for Secure IT Server for Windows, it is not possible for any user to create a new directory in the root directory. UserID must have access to a virtual directory called <code>upload</code> that is mapped to an existing physical directory. ◆ If the server is a UNIX server, creating a new directory at the root level is only possible if UserID has root privileges (not recommended). |
| \$JOB_ID\$-\$FILENAME\$ | <p>Files are created in UserID's SFTP login directory. Filenames use the Job ID followed by a hyphen and the filename of the file on the scanned server.</p> <p>NOTE: Don't prepend text or tokens if you use \$RELATIVE_FILE_NAME\$ with a recursive transfer. Doing this will change both filenames and directory names.</p> |

Related Topics

- ◆ [“Tokens for Job Actions that Transfer Files” on page 55](#)
- ◆ [“Set Up Directory Access on your SFTP Servers” on page 29](#)

- ♦ “Transfer File (Job Action)” on page 78
- ♦ “How to Create and Test Jobs” on page 47

Configure a Job Action that Executes a Command

Job actions are triggered when Reflection Gateway detects new or updated files in a scanned directory. Use this procedure to invoke a command action. You can configure commands that run once or specify a command to act on each file that met the scan conditions.

NOTE: The command runs as a remote SSH command executed using the user account specified for **UserID** on the [New/Edit SFTP Server page \(page 91\)](#). The executable file and output locations must be available to this user. The working directory is the SSH terminal login directory for that user.

To configure a Job action that executes a command

- 1 [Create a Job and specify the scan server and directory.](#)
- 2 On the **New Job** (or **Edit Job**) page, under **Actions**, from the **Add action...** list, select **Execute command**.
This opens the **Execute Command** dialog box.
- 3 For **Options**, select one of the following:
 - ♦ **Run once** executes the command a single time.
 - ♦ **Run for each file** executes the command for each file that has been added or updated since the last scan.
- 4 For **Server**, select the SFTP server on which this command will run.
- 5 For **Command**, specify the command to run and any arguments you want to pass to this command. See [Sample Commands for Job Actions](#) below for examples.
 - ♦ The command runs as a remote SSH command executed using the user account specified for **UserID** on the SFTP server setup page. The executable file and output locations must be available to this user. The working directory is the user’s home directory.
 - ♦ On Windows servers, precede DOS commands with `cmd /c`, for example:

```
cmd /c echo $FILENAME$ >> c:\output\filelist.txt
```
 - ♦ If you include full path information for output, as shown in the example above, the directories in the specified path must exist, and the user who is specified for **UserID** in the file server definition must have access to these directories.
 - ♦ If you do not include full path information for command output, it is created in the terminal session login directory for the user who is specified for **UserID** in the file server definition. On UNIX systems this is typically the home directory (`home/userID`). On the Reflection for Secure IT Server for Windows, this is the user’s Windows Profile directory by default (`c:\users\userID`). This default can be modified from the Reflection for Secure IT Server for Windows console using the Permissions pane.
- 6 Click **OK** to close the **Execute Command** dialog box.
- 7 Click **Save**.
- 8 Click **Run Now** to test the Job. (If this is a repeat test, first update the files in the source location.)

Sample Commands for Job Actions

Use these examples as models for testing and configuring Jobs that execute commands. Samples include appropriate syntax for both Windows and UNIX servers.

Example 1: Run Once

This example uses the `echo` system command and the `$RELATIVE_FILE_LIST$` token to send a list of files on the scanned server that meet the criteria for the Job.

- ◆ **Options** is set to **Run once**
- ◆ **Server** can be the scanned server or a destination server. In this example, the output file (`filelist.txt`) is created in a directory called `output` in the root directory of the selected server. The user account specified for authenticating to this server must have write access to this directory.

Windows SFTP server

Command: `cmd /c echo $RELATIVE_FILE_LIST$ >> c:\output\filelist.txt`

UNIX SFTP server

Command: `echo $RELATIVE_FILE_LIST$ >> /output/filelist.txt`

Example 2: Run for each file

This example uses a script to create a text file that lists token values for each transferred file. The action runs on the destination server after a transfer Job action has copied files to this server.

- ◆ Files have been transferred to a directory called `upload` in the root directory of the destination server. The script is in a directory called `script` on the same server, and output of the script is created in the `script` directory. The user account specified for this SFTP server must have write access to both `upload` and `script`.
- ◆ **Options** is set to **Run for each file**
- ◆ **Server** is set to the destination server name.
- ◆ File tokens are passed to the script as command line arguments. Because the returned values of these tokens can include spaces and special characters, the arguments are enclosed in double quotes.

Windows SFTP server

`c:\script\tokenoutput.bat "$FILENAME$" "$FULL_PATH$" "$RELATIVE_FILE_NAME$"`

Contents of `tokenoutput.bat`:

```
echo FILENAME:      %1 >> c:\script\tokenvalues.txt
echo FULL_PATH:    %2 >> c:\script\tokenvalues.txt
echo RELATIVE_PATH: %3 >> c:\script\tokenvalues.txt
echo ===== >> c:\script\tokenvalues.txt
```

UNIX SFTP server

`/script/tokenoutput.sh "$FILENAME$" "$FULL_PATH$" "$RELATIVE_FILE_NAME$"`

Contents of `tokenoutput.sh`:

```
echo FILENAME:      $1 >> /script/tokenvalues.txt
echo FULL_PATH:    $2 >> /script/tokenvalues.txt
echo RELATIVE_PATH: $3 >> /script/tokenvalues.txt
echo ===== >> /script/tokenvalues.txt
```

NOTE: The script file must have execute permissions set. For example:

Related Topics

- ♦ [“Tokens for Job Actions that Execute Commands” on page 55](#)
- ♦ [“Set Up Directory Access on your SFTP Servers” on page 29](#)
- ♦ [“Execute Command \(Job Action\)” on page 79](#)
- ♦ [“How to Create and Test Jobs” on page 47](#)

Notes for Testing Job Actions

Note the following as you develop Job actions:

- ♦ Use the Reflection Gateway Administrator and Reflection Hub `server.log` for troubleshooting. See [“Job Troubleshooting” on page 100](#) for additional troubleshooting help.
- ♦ You can use the **Run Now** button regardless of State (Enabled or Disabled). This enables you to ensure that the Job actions perform as expected before setting up the scan interval and enabling the Job.
- ♦ A **Run Now** test won't trigger Job actions if the scan directory contents have not changed since your last test. For testing repeatedly from the same directory, you can use the following commands to update the timestamp on all files in a directory:

On UNIX, from a terminal window:

```
touch *
```

On Windows, from a command window

```
copy *.* +,,
```

- ♦ Use `cmd /c` before DOS commands to run on a Windows server. The `/c` switch specifies that `cmd` should exit after the specified command is carried out. For example

```
cmd /c echo $FILENAME$ >> filelist.txt
```
- ♦ Job actions configured using **Execute Command** run on the specified server as a remote SSH command. The command is executed using the user account specified for the **UserID** ([page 91](#)) of that server. This user must have access to all directories required by the command. When `$RELATIVE_FILE_NAME$` or `$FILENAME$` are used with no preceding path information, output is directed to the terminal login directory for that user. For more information see [“Set Up Directory Access on your SFTP Servers” on page 29](#).
- ♦ Job actions configured using **Transfer File** use the SFTP directory access for the **UserID** ([page 91](#)) for the specified server. When `$RELATIVE_FILE_NAME$` or `$FILENAME$` are used with no preceding path, output is directed to the SFTP login directory for that user. For more information see [“Set Up Directory Access on your SFTP Servers” on page 29](#).
- ♦ If you modify settings on an SFTP Server that affect SFTP directory access, you may not see the effects of your changes when you rerun the Job. This is because the Hub maintains and reuses existing connections to SFTP servers for up to 3 minutes of inactivity. (This improves performance because a typical scan requires multiple connections to the scanned server. It also helps improve the performance of Job actions that transfer multiple files.) To ensure that your Job action reflects changes made to the SFTP server configuration, either restart the Reflection Hub service or wait at least 3 minutes after all active scans and Job actions are complete.

- ♦ The **Transfer Site base directory** specified in the SFTP server definition is used for Transfer Sites only. It does not affect the output locations for Job actions.
- ♦ The **Actions** tab in Gateway Administrator is used for configuring Post Transfer Actions only. These actions can be associated with Transfer Sites and run after successful uploads from a transfer client. They are not associated with Jobs. Job actions are configured using the **Transfer File** and **Execute Command** dialog boxes, which are accessible from the **Jobs** tab.

Job Tokens

- ♦ [“Tokens for Job Actions that Transfer Files” on page 55](#)
- ♦ [“Tokens for Job Actions that Execute Commands” on page 55](#)

Tokens for Job Actions that Transfer Files

The tokens described below are available for configuring Job actions that transfer files.

- ♦ For each Job action, tokens that specify a filename or path are generated for each new or updated file in the scanned directory.
- ♦ For sample expressions using these tokens, see [“Entering Expressions for Destination Files” on page 50](#).

| Token | Description |
|------------------------|--|
| \$FILENAME\$ | The name of the file on the scanned server. myfile.txt |
| \$JOB_ID\$ | A unique numeric ID assigned to each Job. |
| \$JOB_NAME\$ | The descriptive Name specified in the New/Edit Job page. |
| \$RELATIVE_FILE_NAME\$ | The path and filename of the file relative to the scanned directory on the scanned server. subdir/myfile.txt |
| \$SCANNED_PATH\$ | The fully-qualified scanned directory on the scanned server. (This is the location specified under Source Files > Directory in the Job definition). /home/scanfiles |

Related Topics

- ♦ [“Configure a Job Action that Transfers Files” on page 50](#)
- ♦ [“Entering Expressions for Destination Files” on page 50](#)
- ♦ [“Transfer File \(Job Action\)” on page 78](#)

Tokens for Job Actions that Execute Commands

Tokens can be used to pass arguments to commands that you specify for Job actions. You can type token values or select tokens using the **Tokens** buttons.

The tokens available depend on whether **Options** is set to **Run once** or **Run for each file**.

For sample commands using tokens, see [“Sample Commands for Job Actions” on page 52](#).

Run once

The following tokens are available when **Options** is set to **Run once**.

| Token | Description |
|--------------------|--|
| DATE | The date of the action on the system running Gateway Administrator. |
| JOB_ID | A unique numeric ID assigned to each Job. |
| JOB_NAME | The descriptive Name specified in the New/Edit Job page. |
| RELATIVE_FILE_LIST | A list of files – including relative path information – that meet the scan criteria. |
| TIME | The time of the action on the system running Gateway Administrator. |
| TIMEZONE | The time zone of the system running Gateway Administrator. |

Run for each file

The following tokens are available when **Options** is set to **Run for each file**.

| Token | Description |
|--------------------|---|
| DATE | The date of the action on the system running Gateway Administrator. |
| FILENAME | The name of the file on the scanned server. <code>myfile.txt</code> |
| FILE_PATH | The fully qualified path to the file on the scanned server – without the filename. <code>/scandir/subdir/</code> |
| FILE_SIZE | The file size (in bytes). |
| FULL_PATH | The fully qualified path – including the filename – of the file on the scanned server. <code>/scandir/subdir/myfile.txt</code> |
| JOB_ID | A unique numeric ID assigned to each Job. |
| JOB_NAME | The descriptive Name specified in the New/Edit Job page. |
| RELATIVE_FILE_NAME | The path and filename of the file relative to the specified scan directory on the scanned server. <code>subdir/myfile.txt</code> |
| TIME | The time of the action on the system running Gateway Administrator. |
| TIMEZONE | The time zone of the system running Gateway Administrator. |

Related Topics

- ◆ [“Execute Command \(Job Action\)” on page 79](#)

6 Managing Transfer Sites

Use Transfer Sites to configure secure file exchange with business partners and employees working outside your corporate network. Transfer Site features include:

- ◆ Integrated web-based Transfer Client

This web-based client provides an easy drag-and-drop interface for transferring files or entire directories. You can customize the Transfer Client to use branding and images that identify your organization.

NOTE: Using the Reflection Transfer Client to access Transfer Sites is not a requirement. Reflection Gateway users can also use the Reflection for Secure IT Secure Shell client, the Reflection FTP Client configured for SFTP transfer, or any other SFTP-enabled SSH client.

- ◆ End-to-end encryption

All transfers are securely encrypted. In addition, when you set up a back-end Transfer Site file server, encrypted data streams continuously through the Reflection Gateway Proxy, eliminating the need to save files on the proxy. This is more secure and more efficient than file transfer solutions that require the file to be stored and then forwarded.

- ◆ Configurable Transfer Site access

Transfer site managers can provide access rights to users or groups and control how long sites remain active. Permissions settings are available to specify who can upload and/or download files and who receives email notifications.

- ◆ Self-registration by email

New external users can be notified via email with links provided for password creation. Customizable email templates are available for account creation, password reset, Transfer Site access notifications, and file upload and download notifications.

- ◆ Manage files after a transfer

You can use either Post Transfer Actions or Jobs to trigger automated processes after files are uploaded to your server. See [“Comparing Jobs and Transfer Sites” on page 14](#).

- ◆ File Transfer auditing

Use audit logging to maintain a complete record of all file transfer activity.

In this Chapter

- ◆ [“How to Create Transfer Sites and Transfer Files” on page 58](#)
- ◆ [“Post Transfer Actions” on page 64](#)

How to Create Transfer Sites and Transfer Files

The procedures in this section are geared to users who are members of the default File Transfer Administrators group, or other groups with the **Manage transfer sites** role enabled. These procedures assume [initial configuration \(page 25\)](#) has already been completed by a Reflection Gateway administrator.

- ◆ [“Connect to Gateway Administrator” on page 58](#)
- ◆ [“Create a Transfer Site” on page 58](#)
- ◆ [“Start the Transfer Client” on page 60](#)
- ◆ [“The Transfer Client User Interface” on page 61](#)
- ◆ [“Use Quick Add to Add Transfer Sites and Users” on page 62](#)
- ◆ [“Transfer Files using an Alternate SFTP Client” on page 63](#)

Connect to Gateway Administrator

Gateway Administrator is a web-based application that you can use to manage users and Transfer Sites.

Before you begin

- ◆ Know the address of the server running Reflection Gateway Administrator
- ◆ Have login credentials for an account that is a member of the File Transfer Administrators group, the Administrators group, or any group with the **Manage transfer sites** role enabled.

To connect to Gateway Administrator

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

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

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

Create a Transfer Site

The procedure below for adding a transfer uses the **New Transfer Site** page. This page provides full access to all Transfer Site configuration options. (If you want to exchange files with a single other user, you can also use [Quick Add \(page 62\)](#) to create a Transfer Site.)

Before you begin

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

To create a Transfer Site

- 1 [Connect to Gateway Administrator \(page 58\)](#).

2 From the **Transfer Sites** tab, click **Add** to open the **New Transfer Site** page.

3 Configure transfer directories.

Transfer site name: This is the folder name users see in their client.

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

4 (Optional) Configure email notification. (To support email notification, [email settings \(page 111\)](#) must be configured by a Reflection Gateway system administrator.)

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

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

5 (Optional) Assign [“Post Transfer Actions” on page 64](#).



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




6 Add one or more users to the site. Users you add will see this site when they connect from their client.

Existing User: Use this area to add existing users or groups to the Transfer Site. They can be in the ReflectionGateway directory, or in any additional LDAP directory that has been added by the Reflection Gateway system administrator.

New Reflection Gateway User: Use this area to create new Reflection Gateway users. New users are sent an account creation email in addition to a Transfer Site access email when you save this site. (This option might not be visible. You must have the [Manage Reflection Gateway users](#) role enabled to view this area.)

7 (Optional) Configure email notification and user permissions.

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

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

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

8 Click **Save**.

Related Topics

- ◆ [“New/Edit Transfer Site” on page 74](#)
- ◆ [“Start the Transfer Client” on page 60](#)
- ◆ [“Transfer Files using an Alternate SFTP Client” on page 63](#)

- ♦ “The Transfer Client User Interface” on page 61
- ♦ “Transfer Client Troubleshooting” on page 101

Start the Transfer Client

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

- ♦ Use links in email messages sent from Reflection Gateway.
- or-
- ♦ From a web browser, enter the following URL, replacing *<Reflection_proxy_host>* with the name or IP address of the Reflection Secure Shell Proxy host.

```
https://<Reflection_proxy_host>:9492
```

-or-

- ♦ Administrators with access to the system on which the Reflection Transfer Server is running can also launch the Transfer Client from the Windows Start Menu (or Apps list). It is installed under **Micro Focus Reflection for Secure IT Gateway > Reflection Transfer Client**.

Warning Messages

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

- ♦ Browser certificate warning

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

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

- ♦ Browser permission to run Java

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

- ♦ Java certificate warning

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

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

- ♦ Java confirmation messages

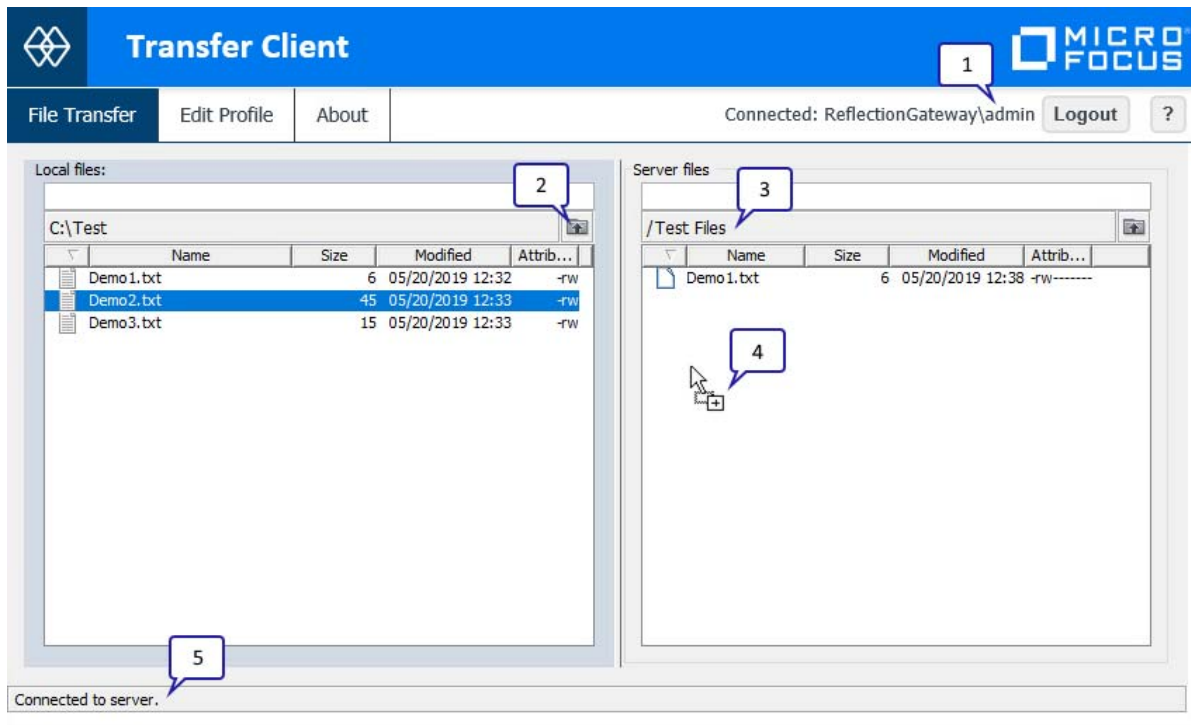
Java uses security messages to ensure that only software you approve runs on your system. These messages identify the publisher of the application and include a "Do not show this again" option.

Related Topics

- ♦ ["Server Certificate Management" on page 131](#)

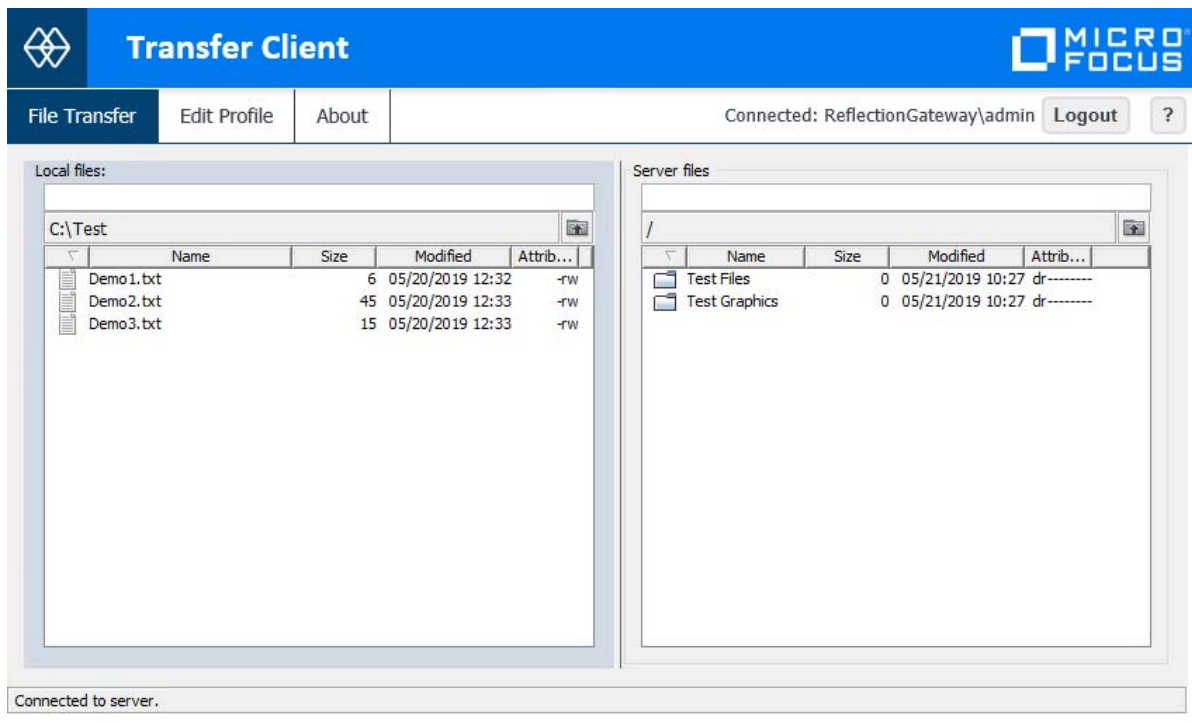
The Transfer Client User Interface

This sample Transfer Client connection points out key features of the Reflection Transfer Client user interface:



1. Logged in user name
2. Use the folder icon to navigate in the file structure
3. Transfer site name
4. Use drag-and-drop to transfer files
5. The status line shows a successful connection

This image shows a connection made by a user with access to two Transfer Sites:



Multiple transfer sites are visible as separate folders when you log in. Double-click a folder to transfer files to or from a site.

Use Quick Add to Add Transfer Sites and Users

Use the **Quick Add** feature to add a new site for a single user using default configuration options. You can add a new user in the same step, or specify an existing user.

To create a user and Transfer Site

- 1 Log on to Gateway Administrator using an account that has the **Manage transfer sites** and **Manage Reflection Gateway users** roles enabled).
- 2 On the **Transfer Sites** page, click **Quick Add**.
- 3 Enter a **Transfer site name**.

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

- 4 Enter a **User email address**.

Each email address is associated with a unique user. When you specify an email address that does not yet exist in the database, the new user will be created with the email address as the UserID. If you enter an existing email, the new Transfer Site is added and made available to that user.

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

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

- 7 **Quick Add** always uses email registration. New users will receive two email messages sent from Reflection Gateway. If you have made no changes to the default email templates, the subject lines say "Your Reflection Gateway User Account" and "Reflection File Sharing: You Have Access to a Transfer Site."

Related Topics

- ♦ ["Start the Transfer Client" on page 60](#)
- ♦ ["The Transfer Client User Interface" on page 61](#)
- ♦ ["Create a Transfer Site" on page 58](#)
- ♦ ["Add Users to the Default User List" on page 35](#)

Transfer Files using an Alternate SFTP Client

Using the Reflection Transfer Client to access Transfer Sites is not a requirement. Reflection Gateway users can transfer files using any other SFTP-enabled SSH client. To use an alternate client, users can connect directly to the Reflection Secure Shell Proxy server (not the Transfer Client URL) as described below.

Before you begin

- ♦ Know the host name or IP address of the Reflection Gateway Proxy (this is the server running the Reflection Secure Shell Proxy).

NOTE: The Reflection Secure Shell Proxy uses port 22 by default. This is the standard SSH port used by most clients. If the proxy has been configured to listen on a different port, the SFTP client will also need to be configured for the correct port.

To use an alternate SFTP client for Reflection Gateway transfers

- 1 Set up the Transfer site from the [New Transfer Site](#) page.

When you are using an alternate client, you need to pay particular attention to the **Send email notification setting**. By default, Transfer Sites are configured to send Transfer Site Access email notifications. The default notifications include a link to the Reflection Transfer Client. To use a different client, do one of the following.

- ♦ Set **Send email notification setting** to **No** and provide users with connection information using some other method.
- OR-
- ♦ Modify the Transfer Site Access email templates to provide users with correct connection information in the notification email.
- 2 Direct users to launch their SFTP client, connect to the server running the Reflection Secure Shell Proxy, and log on using their Reflection Gateway credentials.

For example, this syntax shows how to connect using the Reflection **sftp** command line, which is available in a number of Micro Focus products:

```
sftp gatewayusername@secureshellproxyhost
```

The next procedure describes how to connect using the Reflection FTP Client, which is also included in a number of Micro Focus products.

To configure the Reflection FTP Client for Reflection Gateway transfers

- 1 Start the Reflection FTP Client. This opens the Connect to FTP Site dialog box.
- 2 Click **New**. This launches the connection wizard.
- 3 In **Add FTP Site**, specify the server running the Reflection Secure Shell Proxy.
- 4 In the **Login Information** dialog box, click **Security**. On the **Secure Shell** tab, select **Use Reflection Secure Shell** and click **OK**.
- 5 Continue through the wizard steps. Specifying a user name is optional. If you omit it, you will be prompted for it later.
- 6 Log in using your Reflection Gateway credentials.

Post Transfer Actions

A Post Transfer Action is a program that is invoked on the Transfer Site file server after a file has been successfully uploaded to the server. You can configure Post Transfer Actions in Gateway Administrator or in a Reflection for Secure IT server that has been configured to act as the Transfer Site server.

- ◆ Post Transfer Actions configured in Gateway Administrator

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

NOTE: To use Post Transfer Actions in Gateway Administrator, you must configure the **Transfer site file server** to be an **added SFTP server (page 128)**. Using the Reflection Gateway Proxy (the default) is not supported.

- ◆ Post Transfer Actions in a Reflection for Secure IT Server for Windows.

This approach is available if you have configured a Reflection for Secure IT Server for Windows as your Transfer Site server. Actions configured on this server are not specific to individual Transfer Sites. By default, these Post Transfer actions act on all files uploaded to the server. A filter option is available that enables you to limit the action to all files that match the filter specification. For example, you might configure an Action to act only on files with a `*.exe` extension. This approach is appropriate when you want to ensure that Actions take place after all uploads. A typical use for this kind of Post Transfer Action is running a virus scanner.

NOTE: You can also use Jobs to initiate actions after files are uploaded to a Transfer Site. To compare features of these approaches, see [“Comparing Jobs and Transfer Sites” on page 14](#).

Configure Post Transfer Actions in Gateway Administrator

A Post Transfer Action is a program that is invoked on the Transfer Site server after a file has been successfully uploaded to the server. For example, you might configure an Action in Gateway Administrator that renames or moves successfully uploaded files. Because these Actions are assigned to individual Transfer Sites, you can configure site-specific Actions.

Characteristics of Post Transfer Actions configured on Gateway Administrator:

- ◆ Post Transfer Actions run on the Transfer Site file server.
- ◆ Post Transfer Actions are assigned to Transfer Sites using the **Add Actions** option. An Action will run only if it has been added to the Transfer Site.
- ◆ Although you can assign multiple Actions to a Transfer Site, the order of actions in the Transfer Site definition *does not* control the order of execution for these actions. To ensure that a series of actions takes place in a predictable sequence, it is possible to include the actions in a single script, then create an Action that runs that script. However, using **Jobs** is the preferred approach where multiple actions are required to occur in a specific sequence.
- ◆ Outputs from one Action cannot be used as inputs to another Action.
- ◆ Failed execution of an Action does not prevent other Actions from executing. Use Jobs when you want to ensure that one action is successful before the next action in a sequence is initiated.
- ◆ Actions are executed only after successful transfers. They do not run after unsuccessful or canceled transfers.
- ◆ Post Transfer Actions run immediately after file is transferred. Job actions do not run until after the configured scan interval.
- ◆ Actions are not supported for downloads or other file transfer events, such as renaming or deleting a file on the server.
- ◆ By default, up to 10 Actions can execute simultaneously. Additional actions are added to a queue and executed as other actions are completed. You can modify this default in the Gateway Administrator [properties file \(page 117\)](#) using the **configservice.event.threads** setting.
- ◆ If the Reflection Gateway Administrator service or computer shuts down for any reason, unprocessed actions are processed when the service resumes.

NOTE: To use Post Transfer Actions in Gateway Administrator, you must configure the **Transfer site file server** to be an added SFTP server. Using the Reflection Gateway Proxy (the default) is not supported.

To configure Post Transfer Actions in Gateway Administrator

- 1 Use the **Actions** tab to [define a post transfer action \(page 66\)](#).
- 2 Use the **Transfer Sites** tab to [add the action to a Transfer Site \(page 67\)](#).

Logging for Gateway Administrator Post Transfer Actions

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

```
C:\Program Files\Micro Focus\ReflectionGateway\GatewayAdministrator\logs\
```

Related Topics

- ◆ [“Post Transfer Actions” on page 64](#)

- ◆ [“Post Transfer Action Tokens” on page 70](#)
- ◆ [“Post Transfer Action Troubleshooting” on page 108](#)

Define a Post Transfer Action in Gateway Administrator

You can configure a Post Transfer Action to perform actions on files successfully uploaded to the Transfer Site server.

- ◆ To add or edit Post Transfer Actions, you must be a member of a group with the **Manage actions** role enabled.
- ◆ After an Action is created, it will run only on Transfer Sites that have added it as an action. To add an action to a Transfer Site, you must have the **Manage transfer sites** role enabled; you do not need the **Manage actions** role to add an existing action.

Before you begin

- ◆ In Gateway Administrator's **File Servers** tab, set **Transfer site file server** to be an added SFTP server (not the default setting), and confirm that Transfer Sites can upload successfully to that server.

To define a Post Transfer Action

- 1 [Connect to Gateway Administrator \(page 58\)](#).
- 2 On the **Actions** tab, click **New**.
 - ◆ For **Action name**, specify a descriptive name to identify this action.
 - ◆ For **Command**, specify an executable command or the full path and name of an executable file on the Transfer Site file server followed by command arguments. After the command include any arguments to be passed to the specified program. Arguments can include [supported tokens \(page 70\)](#) (enclosed in dollar signs). Tokens are replaced by actual values when the Action runs. Use spaces to separate multiple arguments. Use double quotation marks around any argument that might include spaces in the returned value.
For examples, see the [Sample Post Transfer Action Commands](#) that follow.
- 3 Click **Save**.
- 4 [Add this Action to one or more Transfer Sites](#).

NOTE

- ◆ If no path information is included, command output is created in the SSH login directory of the user whose **UserID** is configured for authentication in the [server settings \(page 91\)](#) of the Transfer Site file server.
 - ◆ If full path information is included, the destination directory must exist, and the user account specified in the file server settings must be able to write to this directory.
-

Sample Post Transfer Action Commands

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

Example 1: Save token values to a file in the upload directory

This example uses the operating system `echo` command to append the name of the uploaded file and the date of transfer to the contents of a file called `tokenvalue.txt`. (The file is created if it does not exist.) The token `$FILE_PATH$` is used to create this file in the upload directory. Because this destination directory might include spaces, the token is enclosed in double quotation marks.

Windows SFTP server

```
cmd /c echo $FILENAME$: $DATE$ >> "$FILE_PATH$\tokenvalue.txt"
```

NOTE: On Windows servers, precede DOS commands with `cmd /c`. The `/c` switch is required; it specifies that `cmd` should exit after the specified command is carried out.

UNIX SFTP server

```
echo $FILENAME$: $DATE$ >> "$FILE_PATH$/tokenvalue.txt"
```

Example 2: Rename an uploaded file

This example renames the uploaded file by adding the name of the user who uploaded it to the filename. The `$FULL_PATH$` token identifies the full path and name of the uploaded file.

Windows SFTP server

```
cmd /c rename "$FULL_PATH$" "$FILENAME$".$INITIATOR_USERID$
```

UNIX SFTP server

```
mv "$FULL_PATH$" "$FULL_PATH$".$INITIATOR_USERID$
```

Related Topics

- ◆ [“Post Transfer Action Tokens” on page 70](#)
- ◆ [“Configure Post Transfer Actions in Gateway Administrator” on page 65](#)
- ◆ [“Configure Post Transfer Actions in Reflection for Secure IT” on page 68](#)
- ◆ [“Post Transfer Action Troubleshooting” on page 108](#)

Add an Action to a Transfer Site

To run a Post Transfer Action, you need to add the Action to a Transfer Site. After an Action has been added to a Transfer Site, if the Action is enabled (the default), it will act on all files that are successfully uploaded to that site. Post Transfer Actions do not run after uploads to Transfer Sites that have no added actions.

- ◆ To add or edit the Actions associated with a Transfer Site, you must be a member of a group with the **Manage transfer sites** role enabled.

Before you begin

- ◆ One or more Actions must already be [defined \(page 66\)](#).

To add an Action to a Transfer Site

- 1 [Connect to Gateway Administrator \(page 58\)](#).
- 2 On the **Transfer Sites** tab, click **Add** or select an existing site and click **Edit**.

- 3 Use the **Add actions** drop-down list to select the Action you want to add. Added actions appear below the drop-down list. Click the **X** in any added action to remove that action.

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

- 4 Click **Save**.

Related Topics

- ◆ [“Configure Post Transfer Actions in Gateway Administrator” on page 65](#)
- ◆ [“New/Edit Transfer Site” on page 74](#)
- ◆ [“Post Transfer Action Troubleshooting” on page 108](#)

Configure Post Transfer Actions in Reflection for Secure IT

If you have configured Reflection for Secure IT Server for Windows (version 8.2 or later) as your Transfer Site file server, you can set up Post Transfer Actions directly on this server. Unlike Post Transfer Actions created in Gateway Administrator, Post Transfer Actions created this way are not associated with individual Transfer Sites; by default they act on all uploaded files. A typical use for this kind of Action is running a virus scanner.

- ◆ Post Transfer Actions configured on the Reflection for Secure IT server run under the same account as the Reflection for Secure IT service (the Local System account). This account has administrative privileges on the local system.
- ◆ By default, Post Transfer Actions act on all files uploaded to this server. A filter option is available that enables you to limit the action to all files that match the filter specification.
- ◆ You can configure multiple Post Transfer Actions, but the order of actions in the Post Transfer Actions pane *does not* control the order of execution for these actions. To ensure that a series of actions takes place in a predictable sequence, include the actions in one batch file.
- ◆ Outputs from one Post Transfer Action cannot be used as inputs to another Action.
- ◆ Failed execution of a Post Transfer Action does not prevent other Post Transfer Actions from executing.
- ◆ Post Transfer Actions are executed only after successful transfers. They do not run after unsuccessful (or canceled) transfers.
- ◆ Post Transfer Actions are not supported for downloads or other file transfer events (such as renaming or deleting a file on the server).
- ◆ By default, up to 50 actions can execute simultaneously. You can modify this default on the Post Transfer Actions pane.

Logging for Reflection for Secure IT Post Transfer Actions

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

To configure Post Transfer Action logging to a text file on a Reflection for Secure IT Server for Windows

- 1 From the Reflection for Secure IT Server **Configuration** tab, click **Debug Logging**.
- 2 Click **Enable debug logging to log file**. By default, this log is set to **Information**, which is sufficient to include Post Transfer Action output and error messages.
You can click **Custom** to fine-tune the level of output that is sent to this log. Three settings control Post Transfer Action output: LOG_I_PTA_ERROR, LOG_I_PTA_RESULT, and LOG_T_PTA.
- 3 Save your settings (**File > Save Settings**).

To view the text log file

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

Related Topics

- ◆ [“Post Transfer Actions” on page 64](#)
- ◆ [“Post Transfer Action Troubleshooting” on page 108](#)

Define a Post Transfer Action in Reflection for Secure IT

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

Before you begin

- ◆ [Install the Reflection for Secure IT Server for Windows \(page 19\)](#).
- ◆ From the Reflection for Secure IT Server console, [enable debug logging to a text file \(page 68\)](#).
- ◆ Add your Reflection for Secure IT Server to Gateway Administrator and make it the Transfer Site server. Confirm that Transfer Sites can upload successfully to this server.

To configure Post Transfer Actions in the Reflection for Secure IT Server for Windows

- 1 From Reflection for Secure IT Server console, go to **Configuration > Post Transfer Actions**.
- 2 Click **Add** to create a new Post Transfer Action.
For information about configuring **File filter**, **Program**, and **Arguments**, refer to the dialog box help and the [Examples](#) that follow.
- 3 Save your settings (**File > Save Settings**).

Examples

Use these examples as models for testing and configuring Post Transfer Actions in a Reflection for Secure IT Server for Windows.

Example 1: Send a directory listing to the log file

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

File filter: .*

Program: C:\Windows\System32\cmd.exe

Arguments: /c dir "\$FILE_PATH\$"

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

Example 2: Copy uploaded PDF documents to specified directory

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

File filter: .*\.pdf

Program: C:\Windows\System32\cmd.exe

Arguments: /c copy "\$FULL_PATH\$" c:\out

Related Topics

- ◆ [“Post Transfer Action Tokens” on page 70](#)
- ◆ [“Configure Post Transfer Actions in Reflection for Secure IT” on page 68](#)
- ◆ [“Configure Post Transfer Actions in Gateway Administrator” on page 65](#)
- ◆ [“Post Transfer Action Troubleshooting” on page 108](#)

Post Transfer Action Tokens

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

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

The following tokens are available:

| | Description | Sample Output |
|-----------|--|--|
| CLIENT_IP | The IP address of the client system. | fe80::21a5:4df7:fdce:6951 |
| DATE | The date of the transfer. The format for the date is determined by the locale setting of the server. | 05/28/2014 |
| FILENAME | The name of the uploaded file. | myfile.txt |
| FILE_HASH | The SHA-1 hash of the uploaded file. | ebd90566a6a5d7c66a784839cab05b08949a9141 |
| FILE_PATH | The path—without the filename—to the destination directory on the Transfer Site file server. | C:\Base directory\Gateway\transfersite |
| FILE_SIZE | The file size (in bytes). | 7326 |

| | Description | Sample Output |
|----------------------|--|---|
| FULL_PATH | The full path—including the filename—of the destination file on the Transfer Site file server. | C:\Base directory\Gateway\transfersite\myfile.txt |
| INITIATOR_EMAIL * | The email of the client user that uploaded the file. | joe@acme.com |
| INITIATOR_USERID | The domain and user ID of the client user that uploaded the file, in the format: domain\user. | mydomain\joe |
| TIME | The time of the transfer on the Reflection Secure Shell Proxy. | 14:26:59 |
| TIMEZONE | The time zone of the Gateway Administrator server. | -0700 |
| TRANSFER_SITE_NAME * | The Transfer site name from New/Edit Transfer Site (page 74) . | Accounting department files |

* - Supported in Gateway Administrator Post Transfer Actions, but not in Reflection for Secure IT Post Transfer Actions.

Related Topics

- ◆ [“Configure Post Transfer Actions in Gateway Administrator” on page 65](#)

7 Gateway Administrator User Interface

- ◆ [“Transfer Sites” on page 73](#)
- ◆ [“Jobs” on page 76](#)
- ◆ [“Users” on page 80](#)
- ◆ [“Groups” on page 82](#)
- ◆ [“Actions” on page 84](#)
- ◆ [“System” on page 85](#)

Transfer Sites

Use the **Transfer Sites** page to view and manage Reflection Gateway Transfer Sites. Note the following:

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

| | |
|------------------|---|
| Quick Add | Opens the Quick Add dialog box. This provides a quick way to create a new Transfer Site and add a user to the site. If the user email you specify doesn't yet exist in the Reflection Gateway LDAP directory, you see a confirmation message asking if you want to add the user. When you OK this message, a registration email is sent to the user. NOTE: To use this option, you must be a member of the File Transfer Administrators group (or any group that has both Manage Reflection Gateway users and Manage transfer sites enabled). |
| Add | Opens New Transfer Site (page 74). This page provides complete site creation options for creating a new Transfer Site. |
| Edit | Available when one site is selected. |
| Delete | Deletes the selected site or sites. |

Related Topics

- ◆ [“Managing Transfer Sites” on page 57](#)

New/Edit Transfer Site

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

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

Site Configuration Options

| | |
|---|---|
| Transfer site name | <p>This name is visible to users of the site when they connect using the Reflection Transfer Client.</p> <p>The site name must be unique. If you specify the name of an existing site, you'll see an error message when you try to save the site.</p> |
| Directory name | <p>The name of the physical directory to be used by this site on the Transfer site file server. This directory is created in the Transfer site base directory configured for this server. By default, this value is filled in automatically with the Transfer Site name when you move your cursor. In most cases, you should use this default. Specify a different folder if you want your transfer to use an existing directory on the file server. Note: This existing directory must be relative to the base directory.</p> <p>The directory name must be unique. If you specify the name of an existing directory, you'll see an error message when you try to save the site.</p> |
| Delete directory when transfer site is deleted | <p>Note: This setting applies only when the Transfer site file server is set to an added SFTP server. Sites on the Reflection Secure Shell Proxy are not deleted, regardless of the value of this setting.</p> <p>When this option is selected, the physical directory on the SFTP server, and any files it contains, are deleted when the Transfer Site is deleted.</p> <p>When this option is not selected (the default), the physical directory and its contents remain on the file server. If a new site is created using the same directory name as a deleted site, users added to the site will be able to view and transfer any files remaining from the deleted site.</p> |
| Description | <p>An optional description of this site. This description can be added to the Transfer site access email using the \$TRANSFER_SITE_DESCRIPTION\$ token.</p> |
| Expires | <p>When set to Yes (the default), the site expires at the specified date. Expired sites remain in the database, but are not available to Transfer Client users. To restore an expired site, reset the expiration date to a future date.</p> <p>The default expiration is 2 years (730 days) after the site is created. This default is configurable in the Gateway Administrator properties file (page 117).</p> |
| Send email notification | <p>When set to Yes (the default), a Transfer site access email is sent to each user added to the site when you save the site.</p> <p>This option must be enabled at the time users are added to the site. Changing this setting from No to Yes will not result in emails to any users who have already been added and saved as members of the site.</p> |
| Custom message | <p>This option is available when Send email notification is enabled. The message entered here replaces the \$CUSTOM_MESSAGE\$ token in the Transfer site access email.</p> |
| Add actions | <p>If Post Transfer Actions (page 85) are available, they appear in this drop-down list. Post Transfer Actions are executed after a successful file upload. They are not available for downloads or unsuccessful transfers.</p> |

Existing User

Under **Existing User**, add existing users or groups to the Transfer Site. They can be in the ReflectionGateway LDAP directory or in any additional LDAP directory that has been added by the Reflection Gateway system administrator.

| | |
|-------------------------------|--|
| LDAP Server | Select the directory that you want to search. |
| Users Groups | Select whether you want to search for users or groups. Type in the text box to initiate a search for users or groups in the selected LDAP server. Note the following: <ul style="list-style-type: none">◆ The results list shows first and last names (if present) and email. Although the userID is also included in the search, it isn't displayed in the results list.◆ The results list is limited to 10 users. If the user is not visible, continue to enter more of the user's name.◆ The user or group you select is not added to the list until you click Add. |
| Add | This button is available after you have specified a valid user or group. Click it to add the user or group to the Transfer Site list. Users or groups you add to this list are added to the Transfer Site when you click Save . |

New Reflection Gateway User

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

NOTE: This feature relies on email registration for new users. [Configure email support \(page 30\)](#) and test email notification before using this option. If email support is not correctly configured, the account is created, but the user will not receive an account creation email. If users are not receiving email messages, see ["Email Troubleshooting" on page 107](#).

| | |
|-------------------|---|
| User email | When you add a user here, the email address also becomes the user's UserID. Required. |
| First name | Optional. |
| Last name | Optional. |
| Add | Adds the new user to the list of Transfer Site members. Users you add to the list this way are added to the Transfer Site and the ReflectionGateway directory when you click Save . |

User / Group

This list shows the currently configured members of the Transfer Site. To remove any member of the list, click the **X** to the left of the user or group name.

| | |
|---------------------|--|
| User / Group | The name of users and/or groups that have been added to this site. |
| LDAP Server | The LDAP server that the user or group is a member of. |

Notifications

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

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



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



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

Permissions

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

Permissions



Click an icon to enable or disable permissions.



The user can upload files to the site.



The user can download files from the site.



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

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

Related Topics

- ◆ [“Managing Transfer Sites” on page 57](#)

Jobs

Use the **Jobs** page to view and manage Reflection Gateway [Jobs \(page 47\)](#).

- ◆ To view the **Jobs** page and manage Jobs, you must be a member of a group with the **Manage jobs** role enabled.
- ◆ From the Jobs tab, use **Add** to open the [New Job page \(page 77\)](#).
- ◆ You can copy existing Jobs to create new Jobs with similar functionality to existing Jobs. All copied Jobs are marked as **Disabled** initially. This ensures that you don't have identical Jobs running simultaneously.

In this Section

- ◆ [“New/Edit Job” on page 77](#)
- ◆ [“Transfer File \(Job Action\)” on page 78](#)
- ◆ [“Execute Command \(Job Action\)” on page 79](#)

Related Topics

- ◆ [“Create a Job” on page 48](#)

- ◆ “Configure a Job Action that Transfers Files” on page 50
- ◆ “Configure a Job Action that Executes a Command” on page 52
- ◆ “Notes for Testing Job Actions” on page 54

New/Edit Job

Getting there

- 1 Log into Gateway Administrator as a member of a group that has the **Manage jobs** role enabled.
- 2 Click the **Jobs** tab.
- 3 Click **New**, or select an existing Job and click **Edit**.

Use this page to specify the directory to be scanned and to configure Job actions to take place when new or updated files are found in the scanned directory.

- ◆ To view the **Jobs** page, you must be a member of a group with the **Manage jobs** role enabled

| | |
|----------------|---|
| Name | A descriptive name for this Job. |
| State | <p>Enabled – Jobs will run on the specified Scan Interval.</p> <p>Disabled – Jobs will not run automatically, but can be run using Run Now.</p> |
| Run Now | <p>When you click this button, Reflection Gateway scans the files in the specified Directory and initiates listed Job actions if new or updated files are found that meet the filter criteria.</p> <ul style="list-style-type: none"> ◆ You can use Run Now when the state is set to either Enabled or Disabled. ◆ Clicking Run Now will not initiate Job actions if no files have changed since the last time you tested. To test updated Job actions, be sure to make modifications to files in the scanned directory. ◆ The Running Job dialog box indicates that the Job has been initiated. It remains open until you close it. You can close it at any time; closing this dialog box has no effect on the running job. |

Source Files

| | |
|----------------------|--|
| Server | Specify the SFTP server whose directory you want to scan. This can be any Windows or UNIX SFTP server that has been added to Gateway Administrator by the Reflection Gateway system administrator. (See “Add File Servers to Gateway Administrator” on page 27). |
| Directory | <p>The directory to be scanned. Reflection Gateway monitors this directory for new or updated files at the specified scan interval.</p> <p>Select Recursive to include all subdirectories in the scan.</p> |
| Scan Interval | Set the frequency of scans, which days of the week scans take place, and when during the day scans take place. |
| Filters | Set which files are to be scanned based on file name and type, size, modification time, and/or the total number of files in the directory. |

Execute failure action at the end of each scan interval if files do not meet filter conditions

Use this option if you want to receive notification when no new or updated files that meet the filter conditions are found in the scan directory.

Actions

Specify one or more Job actions. These take place in the order given. You can use the arrows to the right of the list to edit this order. Job actions can be either of the following:

- ◆ [Transfer files](#)
- ◆ [Execute a command \(page 79\)](#)

NOTE: If your administrator has configured required [preset actions](#), you will also see a **Preset Actions** list on this page. Preset actions run at the beginning of every job. You can view the configuration of these actions, but they are not editable.

Related Topics

- ◆ [“Create a Job” on page 48](#)
- ◆ [“Notes for Testing Job Actions” on page 54](#)

Transfer File (Job Action)

Getting there

- 1 Log into Gateway Administrator as a member of a group that has the **Manage jobs** role enabled.
- 2 Click the **Jobs** tab.
- 3 Click **New**, or select an existing Job and click **Edit**.
- 4 Under **Action**, in the **Add action...** list, select **Transfer file**.

You can copy or move files between any available SFTP servers.

Preserve file attributes

When it is not selected, the destination file's timestamp shows the date and time of the transfer. When it is selected, the transferred file's timestamp is the same as the file on the source server.

From

Specify the source server and files to transfer from this server.

Enter an expression to describe the files to transfer. For most transfers, use `$_SCANNED_PATH$/$_RELATIVE_FILE_NAME$` (the default) for the initial transfer. This will transfer all updated files on the scanned server that meet your filter criteria. If the scan is recursive, this option will also include all subdirectories in that directory. For subsequent transfers, replace `$_SCANNED_PATH$` with the correct actual path for the files on the server you are transferring from.

To

Specify the destination server and filename and path to copy files to on this server. You can combine [tokens](#) with text and/or other tokens.

The default value, `$_RELATIVE_FILE_NAME$` transfers files to the SFTP login directory for the user whose **UserID** is configured for authentication to this SFTP server.

For additional examples, see [“Entering Expressions for Destination Files” on page 50](#).

Add

Use this option to transfer the same file set to additional servers.

Related Topics

- ◆ [“Configure a Job Action that Transfers Files” on page 50](#)
- ◆ [“Tokens for Job Actions that Execute Commands” on page 55](#)

- ◆ [“Notes for Testing Job Actions” on page 54](#)
- ◆ [“Job Troubleshooting” on page 100](#)
- ◆ [“Set Up Directory Access on your SFTP Servers” on page 29](#)
- ◆ [“File Server Groups Tab” on page 92](#)

Execute Command (Job Action)

Getting there

- 1 Log into Gateway Administrator as a member of a group that has the **Manage jobs** role enabled.
- 2 Click the **Jobs** tab.
- 3 Click **New**, or select an existing Job and click **Edit**.
- 4 Under **Action**, in the **Add action...** list, select **Execute command**.

Use a command Job action to run an executable program or operating system command on a specified server.

You can use tokens to pass arguments to the executable program. The tokens available depend on whether **Options** is set to **Run once** or **Run for each file**. For details, see [“Tokens for Job Actions that Execute Commands” on page 55](#).

| | |
|--------------------------|---|
| Run once | Run the specified command a single time. |
| Run for each file | Run the specified command for each file that has been added or updated since the last scan. |
| Command | <p>The command to run on the specified server. You can use tokens to pass arguments to the executable program.</p> <ul style="list-style-type: none"> ◆ The command runs as a remote SSH command executed using the user account specified for UserID on the SFTP server setup page. The executable file and output locations must be available to this user. The working directory is the user’s home directory. ◆ On Windows servers, precede DOS commands with <code>cmd /c</code>, for example: <pre>cmd /c echo \$FILENAME\$ >> c:\output\filelist.txt</pre> ◆ If you include full path information for output, as shown in the example above, the directories in the specified path must exist, and the user who is specified for UserID in the file server definition must have access to these directories. ◆ If you do not include full path information for command output, it is created in the terminal session login directory for the user who is specified for UserID in the file server definition. On UNIX systems this is typically the home directory (<code>home/userID</code>). On the Reflection for Secure IT Server for Windows, this is the user’s Windows Profile directory by default (<code>c:\users\userID</code>). This default can be modified from the Reflection for Secure IT Server console using the Permissions pane. |

See [“Sample Commands for Job Actions” on page 52](#).

Related Topics

- ◆ [“Notes for Testing Job Actions” on page 54](#)
- ◆ [“Tokens for Job Actions that Execute Commands” on page 55](#)
- ◆ [“Managing Jobs” on page 47](#)

- ◆ [“Job Troubleshooting” on page 100](#)
- ◆ [“Set Up Directory Access on your SFTP Servers” on page 29](#)

Users

Use this page to view and manage Reflection Gateway users. These users can log into the Reflection Transfer Client and access any Transfer Sites that they are members of. Users who have been added to a group with **Gateway Administrator roles** enabled can also log into Gateway Administrator.

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

| | |
|--------------------|--|
| LDAP Server | Specifies which LDAP directory to display. The built-in ReflectionGateway directory is available and selected by default. The Reflection Gateway administrator can add additional servers from the LDAP Servers (page 86) tab. |
| New | Opens New User (page 81) tab. Available only when LDAP server is set to ReflectionGateway. |
| Edit | Opens Edit User (page 82) to edit the selected user. Available only when LDAP server is set to ReflectionGateway and only a single user is selected. |
| Delete | Deletes the selected user or users. Available only when LDAP server is set to ReflectionGateway . You cannot delete the administrator account that you are currently logged in as. |
| Filter User | Searches the selected directory for users that contain the entered string. |
| Clear | Removes the filter and lists all users in the selected directory. |

Related Topics

- ◆ [“Add Users to the Default User List” on page 35](#)
- ◆ [“Provision Users from an Added LDAP Server” on page 37](#)

New User

Use this page to add a new user to the built-in ReflectionGateway list.

- ◆ To view the **New Users** page, you must be a member of a group with the **Manage Reflection Gateway users** role enabled.
- ◆ Red asterisks mark required fields.

| | |
|--|---|
| UserID | The user's login name. Required. This can be the same as the user email address. User ID is not case-sensitive. It must be between 1 and 64 characters in length, and cannot contain the characters <> : " \ ? or these character sequences: CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, and LPT9. |
| Email address | Required. |
| First name | Optional. |
| Last name | Optional. |
| Email registration | When you click Save , the new user is sent an Account creation email that includes a time-limited link for setting a password. NOTE: Do not use email registration if you are also adding this user to a Reflection Gateway group that has access to Gateway Administrator. Email registration is not available to these users. Configure email support (page 30) and test email notification before using this option. If email support is not correctly configured, the account is created, but the user will not receive an account creation email. If users are not receiving email messages, see “Email Troubleshooting” on page 107 . |
| Specify password | If you select this option, no email is sent from Reflection Gateway to your users; you need to manually communicate user name and password information. |
| Require password change | After this user logs in with the initial password, the user will be prompted immediately to change the password. |
| Expires | When set to Yes (the default), the user account expires at the specified date. You can disable an account by setting a date in the past. To enable an expired account, set a date in the future. By default, new Reflection Gateway user accounts are set to expire two years after they are created. This default can be changed by editing the Gateway Administrator Properties File (page 117) . |
| Reflection Gateway group membership | Use the selection box to add this user to any available group. Added groups, and the roles the user inherits from these groups, are displayed under the selection box. Group membership is optional. |

Related Topics

- ◆ [“Users” on page 80](#)
- ◆ [“Groups” on page 82](#)
- ◆ [“Managing Users and Groups” on page 35](#)

Edit User

See [New User \(page 81\)](#) for information about items on this page. Note the following differences:

- ◆ You cannot edit the **UserID** on the **Edit User** page.
- ◆ Click **Change Password** to display the password change options.
- ◆ Email notification is not available for edits to user accounts.

Related Topics

- ◆ [“New User” on page 81](#)
- ◆ [“Managing Users and Groups” on page 35](#)

Groups

Use this page to view and manage Reflection Gateway groups. You can use groups to add members to Transfer Sites, to add members to File Server groups, and to configure roles for Gateway Administrator users.

- ◆ The default Administrators group has all roles enabled. In addition, users in this group can see and manage all Transfer Sites. You cannot delete this group, nor can you delete the last member of this group.
- ◆ The default File Transfer Administrators group has **Manager transfer sites**, **Manage Jobs**, and **Manage Reflection Gateway user** roles enabled.
- ◆ To view the **Groups** page, you must be a member of a group with the **System setup** role enabled.
- ◆ To view the groups in an added LDAP directory, select the directory name in the drop-down list next to **LDAP Server**. The group list is read-only for groups in added LDAP directories; these groups are managed on the LDAP server.
- ◆ Click on a column heading to sort the list based on the entries in that column.
- ◆ To select multiple groups, click multiple check boxes, or use Shift+click to select a range of currently visible groups.

| | |
|---------------------|--|
| LDAP Server | Specifies which LDAP directory to display. The built-in ReflectionGateway user list is available and selected by default. The Reflection Gateway administrator can add LDAP directories from the LDAP Servers tab. |
| New | Opens New Group (page 83) . Available only when LDAP server is set to ReflectionGateway. |
| Edit | Opens Edit Group (page 83) . Available only when LDAP server is set to ReflectionGateway and only when a single group is selected. |
| Delete | Available only when LDAP server is set to ReflectionGateway. You cannot delete the Administrators group. |
| Filter Group | Search the selected directory for groups that contain the entered string. |
| Clear | Clears the filter. |

Related Topics

- ◆ [“Creating and Editing Groups” on page 42](#)
- ◆ [“File Server Groups Tab” on page 92](#)

New Group

Use this page to add a new group to the ReflectionGateway directory.

- ◆ To view the **New Group** page, you must be a member of a group with the **System setup** role enabled.
- ◆ You cannot modify the member list from the **New Group** page. You can modify the members list from the **Edit Group** page. Or, add individual users to a group from the **Edit User** page.

| | |
|--------------------|--|
| GroupID | Required. Cannot contain any of the following characters: <>:\?* * |
| Description | Required. |
| Roles | (Optional) Specify which roles (page 43) are available to users in this group. |

Related Topics

- ◆ [“Groups” on page 82](#)

Edit Group

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

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

| | |
|--------------------|--|
| GroupID | GroupID is read-only when you are editing an existing group. |
| Description | Length must between 1 and 256 characters. |
| Roles | (Optional) Specify which roles (page 43) are available to users in this group. |

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

Members

| | |
|-----------------------|--|
| Add Members | Opens Add Members (page 84) , which you can use to add one or more users to the group. |
| Remove | Removes the selected user or users from the group. |
| Filter Members | Enter text in the text box and click Filter Members to search for users. |
| Clear | Clears the filter. |

Related Topics

- ◆ [“Groups” on page 82](#)

Add Members

Getting there

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

Use this page to add members to any group in the built-in ReflectionGateway user list.

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

| | |
|--------------------|--|
| LDAP Server | Specifies which user directory to display. The list of users shows only those users who are not yet members of the group you are editing. |
| Filter User | Search for users in the listed directory using the text you enter in the search box. |
| Clear | Clears the filter and displays all users of the selected directory who are not already members of the group. |

Related Topics

- ◆ [“Groups” on page 82](#)

Actions

NOTE: To use Post Transfer Actions in Gateway Administrator, you must configure the **Transfer site file server** to be an [added SFTP server \(page 128\)](#). Using the Reflection Gateway Proxy (the default) is not supported.

Use this page to view and edit [Post Transfer Actions \(page 64\)](#).

- ◆ To view the **Actions** page, you must be a member of a group with the **Manage actions** role enabled.
- ◆ These actions can be added to Transfer Site definitions. They are not associated with Jobs. Job Actions are configured from the **Jobs** page.
- ◆ Post Transfer Actions run on the Transfer Site file server.

Related Topics

- ◆ [“Configure Post Transfer Actions in Gateway Administrator” on page 65](#)
- ◆ [“Post Transfer Action Tokens” on page 70](#)

New/Edit Action

NOTE: To use Post Transfer Actions in Gateway Administrator, you must configure the **Transfer site file server** to be an [added SFTP server \(page 128\)](#). Using the Reflection Gateway Proxy (the default) is not supported.

Use this page to configure Post Transfer Actions.

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

Action name Specify a descriptive name to identify this Action. The name you specify here is shown in the list of available actions when you configure a Transfer Site.

Command Specify a system command supported on the Transfer Site file server, or the full path and name of an executable file on that server. For examples, see [“Define a Post Transfer Action in Gateway Administrator” on page 66](#).

After the command include any arguments to be passed to the specified program. Arguments can include [supported tokens \(page 70\)](#) (enclosed in dollar signs). Tokens are replaced by actual values when the Action runs.

Use spaces to separate multiple arguments.

Use double quotation marks around any argument that might include spaces in the returned value.

Tokens Click this button to insert a token from a list of [supported tokens \(page 70\)](#).

Related Topics

- ◆ [“Define a Post Transfer Action in Gateway Administrator” on page 66](#)
- ◆ [“Post Transfer Action Tokens” on page 70](#)

System

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

In this Section

- ◆ [“LDAP Servers Tab” on page 86](#)
- ◆ [“Email Server Tab” on page 88](#)
- ◆ [“Email Templates Tab” on page 89](#)
- ◆ [“File Servers Tab” on page 90](#)
- ◆ [“File Server Groups Tab” on page 92](#)
- ◆ [“Hubs Tab” on page 93](#)
- ◆ [“Authentication Tab” on page 94](#)
- ◆ [“PKI Servers Tab” on page 95](#)

LDAP Servers Tab

Getting there

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

ReflectionGateway is the default user list. Use the **Users** tab to add or delete users in this list. Data for these users is stored in the Reflection Gateway database. You cannot remove this list.

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

Use the selection box on to edit or delete an added server. (The selection box has no affect on user access.)

Windows Active Directory is the only LDAP directory type supported in version 1.1.

New/Edit LDAP Servers Tab

Getting there

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

Use this page to configure connections to an LDAP server.

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

| | |
|--------------------|---|
| Type | Active Directory. This is not configurable; Windows Active Directory is the only LDAP directory type that is currently supported. |
| Domain name | The domain name for this LDAP server. |
| Server | LDAP Server address. This can be a specific server name (<code>myserver.mydomain.com</code>), an IP address (<code>10.10.123.123</code>), or the domain address (<code>mydomain.com</code>). |
| 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 the default global catalog ports is recommended for better performance. For connections without using global catalog, 389 is standard for non-secure connections and 636 is standard for secure connections. |

| | |
|---------------------------------|---|
| Advanced domain settings | <p>Clicking Advanced domain settings expands the display to show the following options. Use these settings to customize how Reflection Gateway manages user authentication to this LDAP server. For additional information, see “LDAP Server Advanced Domain Settings” on page 40.</p> <p>Advanced domain settings apply to password authentication only; X.509 certificate authentication always requires user mapping that specifies both a domain and username.</p> <p>Domain mappings</p> <p>If you have multiple LDAP servers configured, you can use this option to map the value in Domain name to these servers. This can improve performance, because Reflection Gateway authenticates first against the servers you specify here.</p> <p>Remove user domain</p> <p>When set to Yes, any domain name the user enters at login is removed before Reflection Gateway authenticates the user to this LDAP server. For example, if a user enters <code>acme\joe</code>, the domain name <code>acme</code> is removed. If no Default user domain is specified, only the user ID <code>joe</code> is sent to the server for authentication.</p> <p>Default user domain</p> <p>Specifies a default domain name to include when Reflection Gateway authenticates users to this LDAP server. For example, if you specify <code>domain1</code> and a user logs in as <code>user_name</code>, the user is authenticated as <code>domain1\user_name</code>. This can be used in combination with Remove user domain to replace any domain name that the user includes with the value you specify here.</p> |
| UserID | <p>Name of a user who has read access to this LDAP directory.</p> <p>NOTE: You must include the user's domain. For example:</p> <pre>mydomain\user user@mydomain user@mydomain.com</pre> |
| Password | <p>The LDAP user's password</p> |
| Base DN | <p>The base DN under which users are located.</p> <p>For example:</p> <pre>OU=Users,DC=mydomain,DC=com</pre> |
| LDAP Filter | <p>(Optional) Limits the list of users added to Gateway Administrator to those included in the specified filter. If no filter is specified, all users in the specified Base DN are added.</p> <p>Use standard LDAP filter syntax. This example retrieves users in the group <code>myGroup</code>:</p> <pre>((&(objectCategory=user)(memberOf=CN=myGroup,OU=Users,DC=mydomain,DC=com)) (&(objectCategory=group)(CN=myGroup)))</pre> |
| Secure Connection | <p>Select this option to connect to the server using LDAP over SSL (LDAPS).</p> <p>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.</p> |

Related Topics

- ◆ [“Provision Users from an Added LDAP Server” on page 37](#)
- ◆ [“Add LDAP Users to the Administrators Group” on page 39](#)

Email Server Tab

Getting there

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

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

| | |
|----------------------------|---|
| Test Connection | <p>Tests whether the specified SMTP server can be reached at the specified port.</p> <p>This test does not confirm that outgoing messages will be successful. After your email server configuration is complete, you can use the Preview feature on the Email Templates (page 89) page to test an outgoing email.</p> <p>This tests the current on-screen settings. These settings are not saved until you click Save.</p> |
| Save | <p>Saves the current settings. This button is not enabled until you have entered all required information.</p> <p>Certificate information is saved automatically, but other edits are not saved until you click Save.</p> <p>Moving to a new page without clicking Save cancels your edits.</p> |
| Email Service | <p>Select Enabled to enable email emails from Gateway Administrator.</p> |
| SMTP server | <p>The name or IP address of the outgoing email server.</p> <p>This field and the other items on this page cannot be edited if Email service is Disabled.</p> |
| Port | <p>The listening port on the SMTP server.</p> <p>This setting changes automatically when you change the Secure connection setting to match the standard port for each option. If your server uses a non-default port, change the port value after selecting your secure connection type.</p> |
| UserID Password | <p>Some SMTP servers require user credentials to support sending outgoing messages. Use these fields to enter valid user credentials.</p> |
| Sender address | <p>Sets the global default for the sender address that appears in emails sent from Reflection Gateway. This value replaces the \$GLOBAL_SENDER_ADDRESS\$ token.</p> <p>Depending on your email server configuration, you might need to use a valid email account, or you might be able to specify an arbitrary address such as noreply@gateway.com.</p> |
| Sender name | <p>Sets the global default for the user name that appears in emails sent from Reflection Gateway. This value replaces the \$GLOBAL_SENDER_NAME\$ token.</p> <p>Some email servers might ignore this and use the actual name associated with the specified sender address.</p> |

Related Topics

- ◆ [“Configure Email Support in Gateway Administrator” on page 30](#)
- ◆ [“Email Troubleshooting” on page 107](#)

Email Templates Tab

Getting there

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

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

| | |
|------------------------|--|
| <i>Template list</i> | Use this drop-down list to select the template you want to edit. See “Transfer Site Email Notifications” on page 112 for a description of when each template is used. |
| <i>User type</i> | Select Reflection Gateway user to customize templates that are sent to users added to the ReflectionGateway LDAP server. Select LDAP server to edit templates sent to users in an added LDAP server. The default templates are the same for both groups, with the exception of the Password Request template. NOTE: Account Creation and Password Reset are not available for LDAP users. |
| Import | Opens a browse dialog box that you can use to import content from a file created with a text or HTML editor. |
| Restore Default | Restores the default content for the selected template. |
| Sender address | Emails that use the selected template will show that they are from this email address. You can use the default token or delete the token and enter an email address here. Some email servers require that this be a valid user. The GLOBAL_SENDER_ADDRESS token enters the Sender address value specified in the Email Server tab. |
| Sender name | Emails that use the selected template will show that they are from this user. The GLOBAL_SENDER_NAME token enters the Sender name value specified in the Email Server tab. |
| Subject | The subject line that will appear in the email. |
| Insert token | Use this list to insert a token (page 114) in the current cursor position in the message body. Tokens must be preceded and followed by a dollar sign (\$). The dollar signs are added automatically when you use insert token . You can also type token values manually. The list shows the tokens that are supported for the currently selected template. Tokens for which no value is available are omitted from email messages. |
| <i>Body of message</i> | The body can be provided in text or HTML format. You can edit this area directly, or use Import to import content from a file created with a text or HTML editor. |

Preview

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

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

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

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

Related Topics

- ◆ [“Configure Email Support in Gateway Administrator” on page 30](#)
- ◆ [“Email Administration” on page 111](#)
- ◆ [“Customize Transfer Site Email Templates” on page 113](#)
- ◆ [“Email Troubleshooting” on page 107](#)

File Servers Tab

Getting there

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

Use this page to configure SFTP servers to be used for Jobs and/or Transfer Sites. For details about adding and setting up servers, see:

- ◆ [“Add File Servers to Gateway Administrator” on page 27](#)
- ◆ [“Set Up Directory Access on your SFTP Servers” on page 29](#)

Transfer site file server

This setting applies to Transfer Sites only.

Specify the SFTP server to be used for files uploaded to and downloaded from Transfer sites. Files for each Transfer Site you create are placed in a subdirectory of the designated base directory on the file server.

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

Reflection Gateway Proxy

When this option is selected, Transfer Site directories are created on the server running the Reflection Secure Shell Proxy. The default base directory on this server is:

```
C:\ProgramData\Micro Focus\RSecureServer\Reflection\
```

To change the base directory, open the Reflection Secure Shell Proxy console and go to **Reflection Gateway Users > Reflection base path**.

NOTE: If you use Post Transfer Actions, you must select an added SFTP server; Post Transfer Actions are not supported on the Reflection Gateway Proxy.

Related Topics

- ◆ [“Transfer Site Administrative Topics” on page 127](#)
- ◆ [“New/Edit SFTP Server” on page 91](#)
- ◆ [“Set Up the Transfer Site File Server” on page 33](#)

New/Edit SFTP Server

Getting there

- 1 Log into Gateway Administrator as a member of a group that has the **System setup** role enabled.
- 2 Go to **System > File Servers**.
- 3 Click **New**, or select an existing server and click **Edit**.

Added SFTP servers can be used for both Transfer Sites and Jobs.

| | |
|-------------------------------------|--|
| Server | The name or IP address of an SFTP-enabled SSH server. The Reflection for Secure IT Gateway installer includes the Reflection for Secure IT Server for Windows. Each Reflection Gateway license entitles you to install this SFTP-enabled server on one system. Contact Micro Focus for information about purchasing additional Reflection for Secure IT Servers for Windows or UNIX. |
| Port | The port used for SFTP and SSH connections on the server. Port 22 is the standard. |
| Host key fingerprint | Connections to the SFTP server require host authentication using a public key. Once you have specified a server and port, you can click Retrieve to import this key. The host key fingerprint displays the SHA1 hash of the retrieved key. |
| UserID | Specify a valid user account on the SFTP server. Reflection Gateway uses the credentials of this account to access the file system on this server. |
| Password | Select this option to authenticate using a password, and enter the password for the specified user. |
| Public key | Select this option to authenticate using public key authentication. To use this option, public key authentication must be configured for the user on the SFTP server. Copy the user's private key to a location available from the browser, then click Import private key . This imports (copies) the key into the Reflection Gateway database. After the import, you can delete the key from the file system to minimize security risks. |
| Transfer Site base directory | This setting is required only if you want to use this server as your Transfer Site file server. This base directory is not used when the server is configured for Job scanning or Job actions. Specify the base directory under which Reflection Gateway Transfer Site directories will be created. The directory you select must be available to the specified user account. Click Browse to connect to the server and select a location. This automatically enters a path using the correct syntax. By default, the base directory is set to a subdirectory called <code>Reflection</code> in the directory you selected. This is not required; you can edit or delete this subdirectory name. |

Related Topics

- ◆ [“Add File Servers to Gateway Administrator” on page 27](#)
- ◆ [“Set Up Directory Access on your SFTP Servers” on page 29](#)
- ◆ [“Set Up the Transfer Site File Server” on page 33](#)

File Server Groups Tab

Getting there

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

Use File Server Groups to limit which SFTP file servers users have access to when configuring Jobs.

- ♦ File Server Groups limit which servers are visible to users in the **New Job page (page 77)**, the **Transfer File dialog box (page 78)**, and the **Execute Command dialog box (page 79)**.
- ♦ Users who are members of a group with the **System setup** role always have access to all SFTP servers; these users do not need to be a member of a File Server Group.
- ♦ If one or more File Server Groups are configured, users who are members of a group with the **Manage jobs** role enabled (but not **System setup**) must be a member of at least one File Server Group to be able to configure Jobs. These users will only be able to configure Jobs on an SFTP server if they are members of a File Server Group that includes that server.
- ♦ If no File Server Groups are configured, all users with **Manage jobs** rights have access to all SFTP servers when configuring Jobs.

Related Topics

- ♦ [“New/Edit File Server Group” on page 92](#)
- ♦ [“Managing Users and Groups” on page 35](#)

New/Edit File Server Group

Getting there

- 1 Log into Gateway Administrator as a member of a group that has the **System setup** role enabled.
- 2 Go to **System > File Server Groups**.
- 3 Click **New**, or select an existing File Server Group and click **Edit**.

Use this page to add servers and users to File Server Groups.

| | |
|-----------------------------------|---|
| Save | You must include at least one server and one user member to be able to save your group. |
| File server group name | A descriptive name for this group. |
| File servers in this group | Select one or more servers from the list of available servers. To add additional servers, use the File Servers tab. |

Members

Users who are members of this group will be able to configure Jobs using the specified file servers.

| | |
|--------------------|--|
| LDAP Server | Select the directory that you want to search for users to add. |
| Users | Select whether you want to search for users or groups. |
| Groups | Type in the text box to initiate search for users or groups in the selected LDAP server. Note the following: <ul style="list-style-type: none">◆ The results list shows first and last names (if present) and email. Although the userID is also included in the search, it isn't displayed in the results list.◆ The results list is limited to 10 users. If the user is not visible, continue to enter more of the user's name.◆ The user or group you select is not added to the list until you click Add. |
| Add | This button is available after you have specified a valid user or group. Click it to add the user or group to the File Server Group. Users or groups you add to this list are added to the File Server Group when you click Save . |

Related Topics

- ◆ [“File Server Groups Tab” on page 92](#)

Hubs Tab

Getting there

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

Hubs are required to support Reflection Gateway Jobs. If you plan on configuring Jobs, you must add one or more Hubs to this list.

The Reflection Hub service makes connections to SFTP servers and executes the Job actions you have define from the [Jobs page \(page 76\)](#).

You can add multiple Hubs to ensure availability of the Reflection Hub service. If you configure connections to more than one Hub, Reflection Gateway uses a round robin load balancing system to determine which Hub to connect to.

Related Topics

- ◆ [“Add Hubs to Gateway Administrator” on page 30](#)

New/Edit Hub

Getting there

- 1 Log into Gateway Administrator as a member of a group that has the **System setup** role enabled.
- 2 Go to **System > Hubs**.
- 3 Click **New**, or select an existing Hub and click **Edit**.

For most connections you can enter the Hub server name or address and use the default values provided for the other values.

| | |
|---|--|
| State | To disable a hub, click Disabled then Save and Activate . (In this context, this button saves the disabled state, it does not activate the hub.) |
| Save and Activate | This button is available after you have provided required server information. Clicking it does the following: <ul style="list-style-type: none">◆ Confirms that Gateway Administrator can connect to Hub.◆ Configures a certificate on the Hub (if it does not already exist) that will be used by the Hub to authenticate Gateway Administrator in future connections.◆ Retrieves the certificate that will be used by Gateway Administrator to authenticate the Hub in future connections.◆ On the Hub, configures the Gateway Administrator response address and port that will be used by the Hub to send messages back to Gateway Administrator.◆ Saves the Hub address and port in the Gateway Administrator database. |
| Hub server | The host name or IP address that can be used by Gateway Administrator to connect to this Hub. |
| Hub listening port | The port used by Gateway Administrator to connect to the Hub. The default is 9188. This port is configurable on the Hub server in the Hub container.properties file (page 120) using <code>hub.command-api.port</code> . |
| Gateway Administrator server | The host name or IP address of the system running the Gateway Administrator Service. |
| Gateway Administrator listening port | The port used by the Hub to send command responses to Gateway Administrator. The default is 9186. This port is configurable on the Gateway Administrator server in the container.properties file (page 117) using <code>configservice.response-api.port</code> . |
| Certificate information | After a successful connection, this page displays the certificate used by Gateway Administrator to authenticate the Hub. Gateway Administrator automatically trusts the first certificate it receives. To verify the imported certificate, you can compare this information with the certificate in the <code>etc</code> directory on the Hub. If the Hub certificate changes at a later date, delete this Hub configuration and create a new one. |

Authentication Tab

Getting there

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

Use this tab to determine how Transfer Site users authenticate when they connect using the Reflection Transfer Client.

- ◆ The option you select on this page applies to all Reflection Transfer Client users.
- ◆ The option you select on this page does not affect connections from [alternate SFTP clients](#). Users who connect directly to the Reflection Secure Shell Proxy will continue to be able to use password authentication by default. To restrict authentication options for these users, use the authentication settings available from the Reflection Secure Shell Proxy console.
- ◆ Before you can use X.509 certificate authentication, you must have at least one configured PKI Services Manager running, and you need to add it to the Gateway Administrator's **PKI Servers** list. Reflection PKI Services Manager provides certificate verification services, and is available as a separate download from the Reflection for Secure IT Gateway download page at no additional charge. For information about downloading PKI Services Manager and configuring it for use with Reflection Gateway, see [“Set Up PKI Services Manager” on page 45](#).
- ◆ Changes made here require a restart of the Reflection Transfer Server. By default, this restart will occur within one minute after you save your change. (This update interval is configurable in the Reflection Transfer Server [properties file \(page 119\)](#) using the `servletengine.ssl.updateInterval` setting.)

Related Topics

- ◆ [“Configure Certificate User Authentication” on page 44](#)

PKI Servers Tab

Getting there

- 1 Log into Gateway Administrator as a member of a group that has the **System setup** role enabled.
- 2 From Gateway Administrator, go to **System > PKI Servers**.

Reflection PKI Services Manager provides certificate verification services, and is available as a separate download from the Reflection for Secure IT Gateway download page at no additional charge. For information about downloading PKI Services Manager and configuring it for use with Reflection Gateway, see [“Set Up PKI Services Manager” on page 45](#). To support X.509 certificate authentication, at least one PKI Server must be configured.

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

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

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

Related Topics

- ◆ [“Set Up PKI Services Manager” on page 45](#)

- ◆ [“Configure Certificate User Authentication” on page 44](#)
- ◆ [“New/Edit PKI Server” on page 96](#)

New/Edit PKI Server

Getting there

- 1 Log into Gateway Administrator as a member of a group that has the **System setup** role enabled.
- 2 Go to **System >PKI Servers**.
- 3 Do one of the following:
 - ◆ Click **New** to add a new PKI server.
 - ◆ Select a PKI server already on the list and click **Edit**.

Use this page to configure connections to PKI Services Manager. Reflection PKI Services Manager provides certificate verification services, and is available as a separate download from the Reflection Gateway download page at no additional charge. For information about downloading PKI Services Manager and configuring it for use with Reflection Gateway, see [“Set Up PKI Services Manager” on page 45](#).

| | |
|----------------------------|--|
| PKI server | The server running PKI Services Manager. |
| Port | The listening port used by PKI Services Manager. The default (18081) is the default port used by PKI Services Manager. |
| State | New servers are enabled by default. Select Disabled to disable this PKI server without removing it from your list. |
| Retrieve Public Key | Retrieves the public key from the specified PKI server. After you retrieve a key, information about that key is displayed below the button. To compare the retrieved key fingerprint with the actual PKI Services Manager key on the PKI server, start the PKI Services Manager console and go to Utility > View Public Key . |

Related Topics

- ◆ [“Set Up PKI Services Manager” on page 45](#)
- ◆ [“Configure Certificate User Authentication” on page 44](#)

8 Troubleshooting

- ◆ [“Log Files” on page 97](#)
- ◆ [“SFTP File Server Configuration Troubleshooting” on page 99](#)
- ◆ [“Hub Configuration Troubleshooting” on page 99](#)
- ◆ [“Job Troubleshooting” on page 100](#)
- ◆ [“Transfer Client Troubleshooting” on page 101](#)
- ◆ [“Password Troubleshooting” on page 106](#)
- ◆ [“Gateway Administrator Login Page Troubleshooting” on page 107](#)
- ◆ [“Email Troubleshooting” on page 107](#)
- ◆ [“Post Transfer Action Troubleshooting” on page 108](#)
- ◆ [“Server Certificate Troubleshooting” on page 109](#)

Log Files

Review the following for information about working with Reflection Gateway log files:

- ◆ [“Gateway Administrator, Hub, and Transfer Server Logs” on page 97](#)
- ◆ [“Add Debug Logging to the Server Log File” on page 98](#)
- ◆ [“Reflection Secure Shell Proxy Logs” on page 98](#)

Gateway Administrator, Hub, and Transfer Server Logs

Log files for the Reflection Gateway Administrator, the Reflection Hub, and the Reflection Transfer Server are created in the `logs` folders:

```
<install path>\GatewayAdministrator\logs
```

```
<install path>\Hub\logs
```

```
<install path>\TransferServer\logs
```

NOTE: By default, the server log files and debug log files (when debug logging is enabled) roll over daily and are deleted after three days. This helps ensure that disk space is not used up by large, accumulating log files. If you alter the configuration to keep these files for a longer period, you should monitor the files and/or move them to another server to ensure that sufficient disk space is always available.

The following log files are available for the Reflection Gateway Administrator, the Reflection Hub, and the Reflection Transfer Server:

| | |
|----------------------------------|---|
| <code>server.log</code> | This is the principal log file. It rolls over daily. The file called <code>server.log</code> captures log information for the current day. By default, rolled-over log files include the date in year-month-day format, and logs are deleted after three days. |
| <code>server.yyyymmdd.log</code> | |
| | For additional troubleshooting information, you can add debug logging to the Gateway Administrator server.log file (page 98) . |
| <code>debug.log</code> | Debug logging is not enabled by default. A <code>debug.log</code> file is created in the logs folder, but remains empty unless you enable debug logging. The debug log has an hourly rollover set by default, and there is no limit set on the number of old files. |
| | To enable debug logging, see Add Debug Logging to the Server Log File . |

The following additional log is available for the Gateway Administrator:

| | |
|----------------------------|--|
| <code>directory.log</code> | This log is not frequently used. It may be useful for troubleshooting LDAP server access.. |
|----------------------------|--|

Add Debug Logging to the Server Log File

For additional information troubleshooting Jobs, you can log debug information to the Gateway Administrator `server.log` file.

To enable debug logging in the server log file

- 1 As an administrator of the computer running Gateway Administrator, navigate to `GatewayAdministrator\conf` in the Reflection Gateway installation folder. The default location is:

```
C:\Program Files\Micro Focus\ReflectionGateway\GatewayAdministrator\conf
```
- 2 Open `log4j2.xml` file in a text editor.
- 3 Find the "Package level configuration" section:

```
<!-- Package level configurations -->
```
- 4 Add the following line to this section:

```
<logger name="com.attachmate.mft" level="DEBUG" />
```
- 5 Save the `log4j2.xml` file.
- 6 [Restart the Reflection Gateway Administrator service \(page 140\)](#).

NOTE: Edits you make to `log4j2.xml` need to be repeated each time you apply a hotfix or upgrade Reflection Gateway.

Reflection Secure Shell Proxy Logs

The Reflection Secure Shell Proxy supports two methods of logging: to the Windows Event Viewer and/or to a text log file. To configure logging, use the Reflection Secure Shell Proxy console ([Micro Focus Reflection for Secure IT Gateway > Reflection Secure Shell Proxy](#)).

| | |
|----------------------|--|
| Windows Event Viewer | <p>Logging to the Event Viewer is enabled by default.</p> <p>To view the Event Viewer log from the Reflection Secure Shell Proxy console, click the toolbar button, or go to View > Event Viewer.</p> <p>To modify the Event Viewer log level, go to Configuration > Logging > Event logging.</p> |
| Debug (text) logging | <p>Debug logging to text files is not enabled by default.</p> <p>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.</p> <p>To view the log file from the Reflection Secure Shell Proxy console, click the toolbar button, or go to View > Latest Debug Log File.</p> |

SFTP File Server Configuration Troubleshooting

Refer to the following for troubleshooting adding an SFTP server:

Problem: Cannot retrieve Host key fingerprint.

- ◆ Confirm that the server name and port are correct and that the Gateway Administrator has access to this server.
- ◆ Confirm that your firewall configuration allows connections from Gateway Administrator to the SFTP server. See [“Ports and Firewall Configuration” on page 21](#).

Problem: Host key fingerprint is available but **Test Connection** fails.

This indicates a problem with user authentication.

- ◆ Confirm that the username and password (or public key) are correct. If you have access to a different SFTP client, try testing a connection to that server using the same credentials.
- ◆ Confirm that the server is correctly configured to authenticate using the authentication method that you have selected. Most servers accept passwords by default, but server configuration may be changed to require public key authentication.

Hub Configuration Troubleshooting

Use these steps to troubleshoot problems encountered when adding or editing Hubs from the Gateway Administrator **New /Edit Hub** page.

Problem: You see a message saying, **“Failed to activate the hub”** when you click **Save and Activate**.

- ◆ Confirm that the Reflection Hub service is running on the Hub server.
- ◆ Confirm that the Hub server name (or IP address) is correct and that this address is accessible from the Gateway Administrator. If you have modified the Hub listening port, confirm that you specified the correct port. (The default is 9188.)
- ◆ Confirm that your firewall configuration allows connections from Gateway Administrator to the Hub. See [“Ports and Firewall Configuration” on page 21](#).
- ◆ This message may indicate that the certificate used for authentication between Gateway Administrator and the Hub has been modified. To fix this, see [“Reset Server Authentication on a Reflection Hub” on page 141](#).

Problem: You see a message saying, “**Hub certificate was not verified**” when you click **Save and Activate**. You may see this message if you try to re-add a Hub using a different server name or IP address.

- ◆ To resolve this problem restart either the Reflection Hub service or the Reflection Gateway Administrator service.

Problem: The **Disabled** state of a Hub is not saved.

- ◆ To save the disabled state you must click **Disabled** then click **Save and Activate**.

Job Troubleshooting

Review the content in “[Notes for Testing Job Actions](#)” on page 54. This topic summarizes key features that are helpful to new users.

To view log messages, use the Gateway Administrator and Hub `server.log` files.

- ◆ The Gateway Administrator log file is on the system running the Reflection Gateway Administrator service. The default log location is:

```
C:\Program Files\Micro  
Focus\ReflectionGateway\ReflectionGateway\logs\server.log
```

- ◆ The Hub log file is on the system running the Reflection Hub service. The default log location is:

```
C:\Program Files\Micro Focus\ReflectionGateway\Hub\logs\server.log
```

NOTE: If you are running multiple Hubs, Job actions are distributed between the Hubs, and log information for a single Job may be in multiple logs. To simplify troubleshooting, you may want to temporarily disable the other Hubs.

Also review the following troubleshooting guidelines.

Problem: You receive a success notification or see “`step succeeded`” in the server log, but files are not where you expect them to be.

- ◆ Review the information in “[Set Up Directory Access on your SFTP Servers](#)” on page 29. This topic describes where files are created by default for both transfer and command Job actions.

Problem: When you click **Run Now** to test a Job, no files are transferred, no success or failure notifications are sent, and the Gateway Administrator log shows no error messages.

- ◆ Confirm that you have newly modified files in the scan directory. If there have been no changes to the files since your last test (whether it was a success or a failure), no action will be taken.
- ◆ If you want to receive failure notices when no files are found in a scan that meet the scan criteria, on the **New/Edit > Job** page, enable **Execute failure action at the end of each scan interval if files do not meet filter conditions**.
- ◆ To view additional logging, including scan messages, [enable debug logging to the Gateway Administrator server log \(page 98\)](#).

Problem: A file transfer Job fails. If you have a failure action configured, you receive a failure notification.

If the Gateway Administrator server log file includes an ERROR message similar to this:

```
Scanning failed: com.attachmate.mft.hub.fileserver.FileServer Exception: Could not connect to SFTP server.
```

- ◆ The source SFTP server may be down or unavailable.

If the Gateway Administrator server log file includes a WARN message in this format:

```
Failed to open destination file '/path/to/filename' on DestinationServerName:
```

- ◆ The destination SFTP server may be down or unavailable
- ◆ The **UserID** configured for connecting to this SFTP server may not have access rights to the specified destination directory. Review the following information:

[“Set Up Directory Access on your SFTP Servers” on page 29.](#)

[“Entering Expressions for Destination Files” on page 50](#)

Problem: A command execution Job fails. If you have a failure action configured, you receive a failure notification. The Gateway Administrator server log file includes a WARN message saying:

```
One or more command executions failed.
```

- ◆ If you have specified a Windows system command, confirm that the command is preceded by `cmd /c`. For example:

```
cmd /c echo $FILENAME$ >> c:\path\to\output.txt
```

- ◆ If your command directs output to using a fully-qualified path (as shown above), confirm that the user configured for connecting to this SFTP server has access to the location. The command is executed as a remote SSH command using the user account specified for the **UserID** of the server.
- ◆ If you specify a command without including full path information to the executable file, confirm that the executable is on the path of the SFTP server running the command, or is available in the user's login directory.
- ◆ Use an SSH command line client to test your command on the host, as shown here:

```
ssh user@host "command_entered_in_job_action"
```

Transfer Client Troubleshooting

- ◆ [“The Browser Cannot Display the Web Page” on page 102](#)
- ◆ [“Password Login Fails at the Transfer Client Login Page” on page 102](#)
- ◆ [“Transfer Client Login Succeeds but the Server Connection Fails” on page 103](#)
- ◆ [“Server Connection Succeeds but the Transfer Fails” on page 104](#)
- ◆ [“Certificate Authentication Fails” on page 105](#)
- ◆ [“Managing Text File Line Endings” on page 106](#)

Related Topics

- ◆ [“Server Certificate Troubleshooting” on page 109](#)

The Browser Cannot Display the Web Page

Problem: The browser displays a message saying it is unable to display the Transfer Client log in page.

- ◆ Is the Transfer Server running?

Open the Windows Services console and confirm that the Micro Focus Reflection Transfer Server is started.

NOTE: It might take awhile after the service has started in the Windows Services console before you can log in. To confirm that all startup processes are complete, open the Transfer Server [server.log file \(page 97\)](#) and look for "Server Container started."

- ◆ Is the required port open in the firewall?
Check that port 9492 is open inbound on the system running the Reflection Transfer Server.
- ◆ Is the server certificate correctly configured?
See "[Server Certificate Troubleshooting](#)" on page 109.

Problem: The browser displays the message, "HTTP ERROR 403 Problem accessing /webxfer/ui/. Reason: Forbidden"

- ◆ This message may appear if you launch an additional Reflection Transfer Client in a browser session that already has run the Transfer Client. To resolve the issue, close all instances of your browser, then start the Transfer Client.

Password Login Fails at the Transfer Client Login Page

To troubleshoot Transfer Client login issues, use the Transfer Server server log. The default location is:

C:\Program Files\Micro Focus\ReflectionGateway\TransferServer\logs\server.log

Also review the following troubleshooting guidelines.

Problem: The user sees an error message that says, "The username or password you entered is incorrect" or the login page refreshes without displaying any error.

- ◆ Has the user been added to the Gateway Administrator?

In Gateway Administrator, click the Users tab and search each of the configured LDAP servers to confirm that the user exists.

- ◆ If the user exists, is the password correct?

If a user in the ReflectionGateway LDAP server has forgotten the password, you can edit the user in Gateway Administrator to change the password.

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

Connect to Gateway Administrator, go to **System > LDAP Servers**, select your server, click **Edit**, and check the values configured for **Domain Name** and **Advanced domain settings**.

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

- ◆ Is Reflection Gateway user access configured on the Reflection Secure Shell Proxy?

See [“Enable Reflection Gateway Connections in the Reflection Secure Shell Proxy”](#) on page 32.

- ◆ Have configuration changes affected the connection between the Reflection Gateway Proxy and the Gateway Administrator?

On the server running the Reflection Secure Shell Proxy Server, start the server console. On the [Reflection Gateway Users](#) pane, click **Activate and verify**.

Problem: The user sees an error message that says, **"An unknown error has occurred. Please try again later or contact your system administrator."**

- ◆ Are the services running and available?

If you just restarted your Windows computer or just started your Gateway Administrator or the Transfer Server, wait a minute and try again. These services take a few moments to become available.

To confirm that the services are running, on each system, open the Windows Services console and confirm that the Micro Focus Reflection Gateway services are all running.

- ◆ Are required ports open in your firewall?

Check that port 9190 is open from the Reflection Gateway Proxy to the Reflection Gateway Administrator. See [“Ports and Firewall Configuration”](#) on page 21.

- ◆ Have you made configuration changes that affect the connection between the Reflection Gateway Proxy and the Gateway Administrator?

On the Reflection Gateway Proxy, start the Reflection Secure Shell Proxy console. On the [Reflection Gateway Users](#) pane, click **Activate and verify**.

- ◆ Is clustering correctly configured?

If Gateway Administrator servers are configured with different server certificates, users might see this error when they attempt to log in.

Transfer Client Login Succeeds but the Server Connection Fails

The initial login to the Transfer Client succeeds, but the user does not get a successful connection to the server.

Try making a connection using an alternate SFTP client and connect to the Reflection Secure Shell Proxy. (See [“Transfer Files using an Alternate SFTP Client”](#) on page 63.) This helps determine if the problem is with the Reflection Transfer Client and Reflection Transfer Server service or the with the Reflection Secure Shell Proxy.

Refer to the [Reflection Secure Shell Proxy log file \(page 98\)](#) for log 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.

Also review the following troubleshooting guidelines.

Problem: The message **"Loading: <User name>"** is displayed next to the Logout button, but the page below remains empty and/or does not display the available Transfer Sites.

- ◆ Confirm that the latest version of Java is installed on your system and that Java is enabled in your browser.

Problem: The message "**Connection failed: <User name>**" is displayed next to the Logout button and no error message dialog box is displayed.

- ◆ Confirm that the Reflection Secure Shell Proxy service is running. On the Reflection Gateway Proxy server, open the Windows Services console. Confirm that "Micro Focus Reflection Secure Shell Proxy" is started.
- ◆ If you are using a firewall, confirm that port 22 is open inbound to Reflection Gateway Proxy server.
- ◆ If you need to support multiple simultaneous connections, you may have hit the limit of the default **Service account**. Running as the service account (the default) is limited by the operating system to 110 simultaneous client connections. This value is configured from the Reflection Secure Shell Proxy on the **Reflection Gateway Users** pane. Try configuring a **User account**. User accounts do not have this limitation.

Problem: A dialog box appears with the error message "**User authentication failed. Exit Code 14**" or the "**Connecting**" message hangs and is not followed by a successful connection. To troubleshoot these problems, start the Reflection Secure Shell Proxy console.

- ◆ On the **Reflection Gateway Users** pane, confirm that **Allow access to Reflection Gateway users enabled**.
- ◆ On the **Reflection Gateway Users** pane, click **Activate and verify**. The **Web service connection dialog** box will display a series of messages. If the connection is successful, the last message will read "Web service connection has been verified." If you see this message, the configuration changes made might have corrected the problem.
- ◆ If you configured a **User account**, confirm that the credentials are valid. On the **Reflection Gateway Users** pane, click **Select account**. Select the account name, click **Edit**, then click **Test**.
- ◆ Are there permissions settings denying login access? Check the **Permissions** pane and the **Access Control** panes. You can also determine if permission is denied by looking for warning messages in the Reflection Secure Shell Proxy server [log file \(page 97\)](#).

Problem: A dialog box appears with the error message "**Unable to Initialize.**"

- ◆ Are you connecting from a Windows server using Internet Explorer with enhanced security enabled?

Go to **Start > Administrative Tools > Server Manager**. In the Server Manager, click the top node (**Server Manager**) Under **Server Summary**, expand **Security Information**, and click **Configure IE ESC**.

Server Connection Succeeds but the Transfer Fails

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

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

- ◆ Confirm that your Transfer Site file server is running. This message appears if a user attempts to drill down into transfer site directories when the SFTP server is down.

Problem: The user sees an error message that says, "**Unable to execute the file transfer request. The remote directory <directory name> must exist.**"

- ◆ Confirm that your Transfer site file server is running. This message appears if a user attempts to upload a file when the Transfer site file server is down.

Problem: User has difficulty managing drag-and-drop functionality.

- ♦ As an alternative to drag-and-drop, right-click a local file and select **Send file**, or right-click a server file and select **Receive file**.

Problem: The user sees an error message that says, "**The transfer operation to the host has failed or was canceled. Would you like to delete the remote file?**"

- ♦ This message indicates that a transfer is interrupted. Clicking Yes or No determines whether or not a partially uploaded file remains on the server.

Certificate Authentication Fails

Problem: After a user connects to the Transfer Client, the error message says, "**X.509 client authentication is required. Please ensure you are passing a valid X.509 certificate that corresponds to a valid user in the system.**" This message appears when Gateway Administrator is configured to require authentication using X.509 certificates and authentication is not successful. This may be due to any of the following:

- ♦ PKI Services Manager is not running or is not correctly configured in the Gateway Administrator.

Try testing the connection to PKI Services Manager from Gateway Administrator. Go to **System > PKI Servers**. Select your added server, click **Edit**, then click **Verify Connection**.

- ♦ No certificate is available on the client system.

Has the client system been configured to use a smart card or present a personal certificate from the browser's personal certificate store?

- ♦ The certificate is mapped to an invalid user account or is mapped to multiple user accounts.

The PKI Services Manager identity mapping must return a single, valid user for the presented certificate. Use the PKI Services Manager test utility to view allowed identities. (Start the PKI Services Manager console and go to **Utility > Test Certificate**.) The allowed identity list should consist of exactly one user, and that user must be provisioned in Gateway Administrator.

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

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

- ♦ The problem may be in your browser configuration. Try configuring and testing with an alternate browser.

Managing Text File Line Endings

File transfers between the Reflection Transfer Client and the Reflection Secure Shell Proxy Server are always binary. This means that the content of transferred files, including text file line endings, is not modified in any way during the transfer. If you are managing text file transfers from systems that use different line endings (for example Mac or UNIX files transferred to the Windows server), use a text-file conversion utility to modify line endings.

Text file line ending conversion is configurable for file transfers between the [Reflection Secure Shell Proxy \(page 128\)](#) 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 Secure Shell Proxy servers; it will not work with OpenSSH servers.)

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

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

Password Troubleshooting

If email password reset is not working, review the following possible causes.

NOTE: Administrators with the Manage [Reflection Gateway users](#) role can update user passwords from Gateway Administrator. From the **Users** tab, select the user, click **Edit**, then click to expand **Change password**.

Problem: After clicking **Reset** on the password reset page, the user sees a message that says, "**Time sensitive instructions to create a new password have been sent to the email address we have on record for this account...**" but the user does not receive an email

- ◆ Confirm that email support is correctly [configured \(page 30\)](#) in Gateway Administrator.
- ◆ Because the Gateway Administrator provides access to sensitive information, users who are members of any group with access to the Gateway Administrator cannot reset their password using the Transfer Client reset link. These users *will not* receive any email notification after clicking the link. Users with the [Manage Reflection Gateway users](#) role can reset their password using Gateway Administrator. Gateway Administrator users who do not have this role should contact a member of the Administrators or File Transfer Administrators group.

Problem: After clicking **Reset** on the password reset page, the user sees a message that says, "**An unknown error has occurred. Please try again later or contact your system administrator.**"

- ◆ This indicates that the connection to the Transfer Service failed. The log might include the message "Authentication failed for user rsitmodule."

To resolve this, open the Reflection Secure Shell Proxy. On the [Reflection Gateway Users](#) pane, click **Activate and Verify**.

Gateway Administrator Login Page Troubleshooting

Problem: The browser is unable to display the Gateway Administrator log in page.

- ◆ Is the Gateway Administrator service running?

Open the Windows Services console and confirm that the Micro Focus Reflection Gateway Administrator service is started.

NOTE: It might take awhile after the service has started in the Windows Services console before you can log in. To confirm that all startup processes are complete, open the Gateway Administrator [server.log file \(page 97\)](#) and look for "Server Container started."

- ◆ Is the required port open in the firewall?
Check that port 9490 is open inbound on the system running the Gateway Administrator.
- ◆ Is the server certificate correctly configured?
See "[Server Certificate Troubleshooting](#)" on page 109.

Problem: There is no "Forgot password?" link on the Gateway Administrator login page.

- ◆ Email password reset is not available for Gateway Administrator users. This is by design to help ensure the security of Gateway Administrator data.

Email Troubleshooting

To troubleshoot email problems, use the Gateway Administrator `server.log` file. The default location is:

```
C:\Program Files\Micro  
Focus\ReflectionGateway\GatewayAdministrator\logs\server.log
```

Also review the following troubleshooting guidelines:

Problem: No email is being sent.

- ◆ To test the email server connection, go to **System > Email Server** and click **Test Connection**. If this test fails, confirm the **SMTP server** and **Port** values.
- ◆ After you confirm that the email server connection is working, try sending a test email. Go to **System > Email Templates** and click **Preview**. Enter your email address in the **To:** field and click **Send Test Email**. If this fails, see the next item.

Problem: The email server connection succeeds, but test email sent from the **Email Templates** page fails.

- ◆ The sender name or address might be invalid. Open the **Preview** option and try replacing the token used for **Sender address** email with a valid email address for your server. If this fixes the problem, go to the **Email Server** page and replace the global **Sender address** on this page, or edit the template to use the valid address instead of the token.
- ◆ Your server may require a valid user and password. If you omitted **UserID** and **Password** on the **Email Server** tab, enter valid credentials and test again.
- ◆ Confirm that the **Email Server** settings for **Secure connection** meet the requirements of your email server.

Problem: The link in a Reflection Gateway email leads to a web page not available error.

- ◆ Does the URL in the email point to "localhost" (https://localhost:9492/webxfer/recovery.jsp)? This indicates that the base URL has not been updated from the default. Open the [“Gateway Administrator Properties File” on page 117](#), edit the value of **transfer.server.url**, and restart the Reflection Gateway Administrator service. For details, see [“Configuring the URL for Transfer Site Email Messages” on page 31](#).

Problem: Email is generally working, but some specific email messages aren't sent.

- ◆ Confirm that the email address specified for the user is correct. An incorrectly entered email addresses will not result in an error in the console log. This error is handled by the SMTP server. Check for undeliverable mail notifications in the inbox of the user account specified in the **Email Server** tab.
- ◆ User registration email is sent only when a user is first added, not after subsequent edits. If the initial registration email fails because of an incorrect user address, correct the address on the **Edit User** page. You can manually update the password at this time. Or, users who know their user ID but have not yet set a password can create a password by clicking the link in a transfer site access email, and then using the **Forgot password?** option.
- ◆ Because the Gateway Administrator provides access to sensitive information, users who are members of any group with access to the Gateway Administrator cannot reset their password using the Transfer Client reset link. These users *will not* receive any email notification after clicking the link. Users with the **Manage Reflection Gateway users** role can reset their password using Gateway Administrator. Gateway Administrator users who do not have this role should contact a user with rights to manage users.

Problem: Email is not sent in a timely manner, is not sent at all, and/or the server starts showing very high CPU utilization

- ◆ You may have multiple queued email messages that are not being sent or are taking unexpectedly long to send. Check the event queue file (`<install path>\GatewayAdministrator\etc\emailQueue.rnd`). If this file is large (>500 KB), it suggests that failing emails are preventing other emails from being processed. To remove all queued emails, stop the Gateway Administrator service and delete this file.

Post Transfer Action Troubleshooting

Gateway Administrator Post Transfer Action

To view Gateway Administrator Post Transfer Action output and error messages, use the Gateway Administrator `server.log` file and look for entries that include `TransferSiteEventHandler`. The default location is.:

```
C:\Program Files\Micro  
Focus\ReflectionGateway\GatewayAdministrator\logs\server.log
```

Also review the following troubleshooting guidelines:

- ◆ Confirm that you are using an added SFTP server for Transfer Sites, not the default Reflection Gateway Proxy. The Reflection Gateway Proxy is not supported for Post Transfer Actions.
- ◆ If the Post Transfer Action doesn't run, confirm that the action is added to your transfer site.
- ◆ Check the log to see if any resolved arguments include spaces. Use double quotation marks around these tokens.
- ◆ If the log includes syntax errors, check to see if any resolved arguments include unsupported characters.

- ◆ If the log includes the error "Unable to complete Transfer Site action," check to see that the configured name and path specified for the Post Transfer Action program are correct. If the the action configuration includes a full path to the executable program, confirm that the SFTP server user account has rights to access this path.
- ◆ If the log includes permission errors, check to see if the SFTP server user account has permissions to write to locations required by actions defined in the Post Transfer Action.
- ◆ If Post Transfer Actions fail to execute and/or the server starts showing very high CPU utilization, you may have multiple queued Post Transfer Action events that are not completing or are taking unexpectedly long to complete. Check the event queue file (`<install path>\GatewayAdministrator\etc\eventQueue.rnd`). If this file is large (>500 KB), it suggests that events that have not completed are preventing others from being processed. To remove all queued events, stop the Gateway Administrator service and delete this file.

Reflection for Secure IT Post Transfer Actions

To view Reflection for Secure IT Post Transfer Action output and error messages, configure output to the debug (text) log file. For details, see ["Configure Post Transfer Actions in Reflection for Secure IT" on page 68](#).

Also review the following troubleshooting guidelines:

- ◆ Confirm that you saved your server settings after creating or modifying your action and that the action is enabled.
- ◆ If the Post Transfer Action doesn't run, the expression for your filter might be incorrect. Try a test with the default filter (. *).
- ◆ Check the log to see if any resolved arguments include spaces. Use double quotation marks around these tokens.
- ◆ If the log includes syntax errors, check to see if any resolved arguments include unsupported characters.

Server Certificate Troubleshooting

Refer to these troubleshooting steps if you changed the server certificate used by the Transfer Server or Gateway Administrator server.

After any changes you make to server certificate setup, always perform both of the following before retesting:

- 1 Close all browser windows.
- 2 Restart the server whose certificate you are configuring. See ["Start and Stop the Reflection Transfer Server" on page 140](#) and ["Start and Stop the Reflection Gateway Administrator Service" on page 140](#).

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`?
- ◆ Is the keystore file in the location specified for `servletengine.ssl.keystore`?
- ◆ Did you migrate your PKCS#12 or JKS keystore to BCFKS format? See ["Migrate PKCS#12 or JCEKS keystores to BCFKS keystores" on page 135](#).

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 log file.

This exception is most likely to occur if the Transfer Server has not been updated to trust a new Gateway Administrator certificate. To resolve this issue, from the Reflection Secure Shell Proxy console, go to the **Reflection Gateway Users** pane and click **Activate and verify**.

9 Reflection Gateway System Administration

- ◆ [“Email Administration” on page 111](#)
- ◆ [“Configuration and Data Files” on page 116](#)
- ◆ [“Job Administrative Topics” on page 125](#)
- ◆ [“Transfer Site Administrative Topics” on page 127](#)
- ◆ [“Server Certificate Management” on page 131](#)
- ◆ [“Managing the Reflection Gateway Services” on page 140](#)
- ◆ [“Ensuring High Availability of Reflection Gateway Services” on page 143](#)
- ◆ [“Create an Audit Log of File Transfers” on page 150](#)
- ◆ [“Change the JDK” on page 151](#)

Email Administration

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

- ◆ Account creation email for new users
- ◆ Password reset email
- ◆ Transfer site access notification
- ◆ Notification sent to site managers and/or site members when files are uploaded or downloaded
- ◆ Job success and failure notifications sent to job administrators.

In this Section

- ◆ [“Initial Email Setup” on page 111](#)
- ◆ [“Transfer Site Email Notifications” on page 112](#)
- ◆ [“Customize Transfer Site Email Templates” on page 113](#)
- ◆ [“Transfer Site Email Tokens” on page 114](#)

Initial Email Setup





To support email services, you need to:

- ◆ Configure the Gateway Administrator **Email Server** ([page 88](#)) settings.
- ◆ Edit the Gateway Administrator `container.properties` ([page 117](#)) file to include the public-facing URL that will be used in email links.

For detailed procedures, see [“Configure Email Support in Gateway Administrator” on page 30](#).

Transfer Site Email Notifications

Reflection Gateway Transfer Sites support the following email notifications.

| Notification | When is it sent? |
|---|---|
| Account Creation Provides a link for new users to set their password. | Account creation email is sent when: <ul style="list-style-type: none">♦ Users are added using Users > New, and Email registration is selected (the default).♦ Users are added using Transfer Sites > Quick Add.♦ Users are added using Transfer Site > Add (or Edit) > New Reflection Gateway User. Account creation email is not sent when: <ul style="list-style-type: none">♦ Users are added using Users > New, and Specify password is selected.♦ Users are added by adding LDAP servers. |
| Transfer Site Access Provides a link for users to launch the Transfer Client. | Sent by default to users who are added to a Transfer Site, either when it is first created or by edits to an existing site. You can enable or disable this notification for each site from the New/Edit Transfer Site page using Send email notification . |
| File Upload Provides information about each file upload to a site. | Sent when a file is successfully uploaded to a Transfer Site. Upload notification is site-specific and is disabled by default. You can enable notifications for any member of a site from the New/Edit Transfer Site page. Click the icon under Notifications in the member list. Disabled:  Enabled:  |
| File Download Provides information about each file download from a Transfer Site. | Sent when a file is successfully downloaded from a Transfer Site. Download notification is site-specific and is disabled by default. You can enable notifications for any member of a site from the New/Edit Transfer Site page. Click the icon under Notifications in the member list. Disabled:  Enabled:  |
| Password Request Provides a link to the password reset page. | Sent to users who click the Forgot password? link in the Transfer Client login page. <ul style="list-style-type: none">♦ Because the Gateway Administrator provides access to sensitive information, users who are members of any group with access to the Gateway Administrator cannot reset their password using the Transfer Client reset link. These users <i>will not</i> receive any email notification after clicking the link. Users with the Manage Reflection Gateway users role can reset their password using Gateway Administrator. Gateway Administrator users who do not have this role should contact a member of the Administrators or File Transfer Administrators group.♦ LDAP users cannot change their passwords using this reset. These users receive an email message, but it should not include a password reset link. The default template for LDAP users provides an example of an appropriate message to send to these users. |

| Notification | When is it sent? |
|---|---|
| Password Reset | Sent to users who have successfully reset their password. |
| Informs users that their password has been reset. | |

Related Topics

- ◆ [“Initial Email Setup” on page 111](#)
- ◆ [“Customize Transfer Site Email Templates” on page 113](#)

Customize Transfer Site Email Templates

You can customize the content and/or format of the Transfer Site email messages sent from Reflection Gateway Administrator. Your customized content can use either text or HTML format.

Before you begin

- ◆ [“Configure Email Support in Gateway Administrator” on page 30.](#)

To customize an email template

- 1 Log on to Gateway Administrator using an account in the Administrators group (or any account that has the **System setup** role enabled).
- 2 Go to **System > Email templates**.
- 3 Select the template you want to customize. (Account Creation is displayed by default.)
- 4 Select the user pool (Reflection Gateway users or users in an added LDAP server) for this template. Note the following:
 - ◆ If you want to send the same customized email to both user pools, customize the template for each pool in a separate step.
 - ◆ Account Creation and Password Reset are not available for LDAP users.
- 5 (Optional) Customize the **Sender address**, **Sender name**, and **Subject** for this email. The default tokens entered for address and name are replaced with the global values specified in the **Email Server** tab. You can delete these tokens and replace them with an actual address or sender name.
- 6 Edit the message text using any combination of the following techniques. The text can use either text or HTML format.
 - ◆ Edit the text directly in Gateway Administrator. Click **Insert token** to insert a [token \(page 114\)](#) in the current cursor position. This automatically inserts the token with the required dollar signs (\$).
 - ◆ Click **Import** to import content you have created and saved using a text or HTML editor. To add tokens in these editors, type the token name manually, including the required dollar signs.
 - ◆ Copy and paste text into the message body.

- 7 (Optional) Expand the **Preview** feature to preview your email or send a test email. Note the following:
 - ◆ Tokens in the preview are replaced by sample content enclosed in square brackets. For example: [myTransferSite]. In actual generated email, the brackets do not appear and the sample content is replaced by actual content.
 - ◆ To send a test email, enter an email address and click **Send Test Email**. This test can help you determine if your email server is correctly configured and supports your current values for Sender address and Sender name.
- 8 Click **Save**.
- 9 (Recommended) Because the preview email messages do not show how token replacement is actually handled, you should follow up a successful preview test with a test of an actual email notification.

Sample HTML content

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

```
<html>
<font face="Arial, Helvetica, sans-serif">
<p>You have been given access to the following Transfer Site:
<b>${TRANSFER_SITE_NAME$}</b>.</p>
<p>Click here ${TRANSFER_SITE_LINK$} to connect and transfer files.</p>
<p>${CUSTOM_MESSAGE$}</p>
<p>--</p>
<p>Sent from Micro Focus Reflection for Secure IT Gateway</p>
</font>
</html>
```

Related Topics

- ◆ [“Transfer Site Email Notifications” on page 112](#)
- ◆ [“Transfer Site Email Tokens” on page 114](#)

Transfer Site Email Tokens

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

- ◆ Tokens for which no value is available are omitted from email messages.
- ◆ You can use the **Preview** feature on the **Email Templates** tab to see sample token output. To see actual replacement values, send a test email.

The following tokens are supported:

| Token | Description | Available with |
|-------------------------|--|--|
| ACCOUNT_EXPIRATION_DATE | The account expiration date of the user receiving the email. | All |
| CLIENT_IP | The IP address of the client system. | File Upload File Download |
| CUSTOM_MESSAGE | Custom message from New/Edit Transfer Site (page 74) . If no custom message is configured, this token is replaced by an empty string. | Transfer Site Access File Upload File Download |

| Token | Description | Available with |
|-----------------------------|--|--|
| DATE | The date of the action. | All |
| FILENAME | The name of the uploaded or downloaded file. | File Upload File Download |
| FILE_HASH | The SHA-1 hash of the uploaded or downloaded file. | File Upload File Download |
| FILE_PATH | The path—without the filename—to the destination directory (uploads) or source directory (downloads) on the Transfer Site file server. | File Upload File Download |
| FILE_SIZE | The file size (in bytes). | File Upload File Download |
| FIRST_NAME | The first name of the user receiving the email. Note: First name is an optional field for Reflection Gateway users. If no first name is available, this token is replaced by an empty string. | All |
| FULL_PATH | The path—including the filename—to the destination file (uploads) or source file (downloads) on the Transfer Site file server. | File Upload File Download |
| GLOBAL_SENDER_ADDRESS | Sender address from Email Server (page 88) . | All |
| GLOBAL_SENDER_NAME | Sender name from Email Server (page 88) . | All |
| INITIATOR_EMAIL | The email of the action initiator (page 116) . | All |
| INITIATOR_USERID | The user ID of the action initiator (page 116) . For LDAP users, the domain name is included (domain\userID). For Reflection Gateway users, the domain name is omitted (userID). | All |
| LAST_NAME | The last name of the user receiving the email. Note: Last name is an optional field for Reflection Gateway users. If no last name is available, this token is replaced by an empty string. | All |
| PASSWORD_RESET_LINK | The URL that links to the password reset page. The host and port are set in the Gateway Administrator properties file using the transfer.server.url. | All |
| PASSWORD_RESET_LINK_TIMEOUT | The length of time password reset can be accomplished after a reset email is sent. This value is configured in the Gateway Administrator properties file using password.reset.expiration. | All |
| TIME | For uploads and downloads, this is the time on the Reflection Secure Shell Proxy. For all other events, this is the time on the Gateway Administrator. | All |
| TIMEZONE | The time zone of the Reflection Gateway Administrator. | All |
| TRANSFER_SITE_DESCRIPTION | Description from New/Edit Transfer Site (page 74) . Note: Description is an optional field. If no description is available, this token is replaced by an empty string. | Transfer Site Access File Upload File Download |

| Token | Description | Available with |
|--------------------|--|---|
| TRANSFER_SITE_LINK | The URL for connecting to the Transfer Client. The host and port are set in the Gateway Administrator properties file using the transfer.server.url. | Transfer Site Access File Upload File Download |
| TRANSFER_SITE | The Transfer site name from New/Edit Transfer Site (page 74) . | Transfer Site Access File Upload File Download |
| USERID | The User ID of the user receiving the email. For LDAP users, the domain name is included: domain\userID. For Reflection Gateway users the domain name is omitted: userID | All |
| USER_EMAIL | The email address of the user receiving the email. | All |

Action Initiator

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

| In this template: | The action initiator is: |
|----------------------|---|
| Account Creation | User who added the account to the Reflection Gateway Users list |
| Transfer Site Access | User who added the recipient to the Transfer Site |
| File Upload | User who uploaded the file |
| File Download | User who downloaded the file |
| Password Request | User who clicked the "Forgot password?" link |
| Password Reset | User who clicked the "Forgot password?" link |

Configuration and Data Files

In this Section

- ◆ [“Gateway Administrator Properties File” on page 117](#)
- ◆ [“Transfer Server Properties File” on page 119](#)
- ◆ [“Hub Properties File” on page 120](#)
- ◆ [“Reflection Gateway Data Files” on page 121](#)
- ◆ [“Backing Up Gateway Administrator Data” on page 123](#)
- ◆ [“Changing the Gateway Administrator Database” on page 123](#)

Gateway Administrator Properties File

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

```
C:\Program Files\Micro Focus\ReflectionGateway\GatewayAdministrator\conf
```

NOTE

- ◆ You must [restart the server \(page 140\)](#) 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.
-

Database settings

Default settings configure connection to the default HyperSQL database. Commented settings show sample configuration to MySQL. For more information about changing the database, see [“Changing the Gateway Administrator Database” on page 123](#).

jdbc.url

The connection information for the database. Edit `localhost:3306/mft` to specify the host, port, and database name of your database. Do not change `useSSL=false`; SSL connections are not supported.

jdbc.username

The username of a user with access to the database.

jdbc.password

The password of a user with access to the database.

hibernate.dialect

Use the value shown in the file.

ldaps.port.enabled

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

directory.ldaps.port

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

servletengine.ssl.port

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

transfer.server.url

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

password.reset.expiration

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

configservice-ws.host

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

configservice-ws.port

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

Certificate settings

For more information about changing the server certificate, see [“Replace the Default Server Certificate” on page 131](#).

servletengine.ssl.keystore

The path to the keystore that contains the server certificate and private key. The path must be specified using forward slashes or escaped backslashes. For example:

- ◆ C:/path/to/keystore
- ◆ C:\\path\\to\\keystore
- ◆ You can specify a relative or absolute path. The default is ../etc/mycert.bcfks.

servletengine.ssl.keystoretype

The file type of the keystore that contains the server certificate and private key. The only supported Java keystore type is BCFKS.

servletengine.ssl.keystorepassword

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

configservice.event.threads

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

configservice.email.threads

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

configservice.hubevent.threads

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

configservice.account.expiration

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

configservice.transfersite.expiration

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

configservice.response-api.interface

The network interface used by the Hub to send command responses to Gateway Administrator.

configservice.response-api.port

Listening port on Gateway Administrator used by the Hub to send command responses to Gateway Administrator. This value must match the value for **Gateway Administrator listening port** configured on the [Edit Hub page](#).

Related Topics

- ◆ [“Transfer Server Properties File” on page 119](#)
- ◆ [“Server Certificate Management” on page 131](#)
- ◆ [“Ports and Firewall Configuration” on page 21](#)

Transfer Server Properties File

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

```
C:\Program Files\Micro Focus\ReflectionGateway\TransferServer\conf
```

NOTE

- ◆ You must [restart the server \(page 140\)](#) after editing `container.properties` for your changes to take effect.
 - ◆ A backup file, `container.properties.example`, in the same folder provides a copy of the original default settings.
-

servletengine.ssl.port

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

servletengine.ssl.updateInterval

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

Certificate settings

For more information about changing the server certificate, see [“Replace the Default Server Certificate” on page 131](#).

servletengine.ssl.keystore

The path to the keystore that contains the server certificate and private key. 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.bcfks`.

servletengine.ssl.keystoretype

The file type of the keystore that contains the server certificate and private key. The only supported Java keystore type is BCFKS.

servletengine.ssl.keystorepassword

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

sftp.hostname

The hostname used by the Transfer Client to connect to the Reflection Secure Shell Proxy.

sftp.port

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

Hub Properties File

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

```
C:\Program Files\Micro Focus\ReflectionGateway\Hub\conf
```

NOTE

- You must [restart the server \(page 141\)](#) 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.
-

hub.events.threads

Specifies the number of commands to process in parallel. If the number of active commands is under this limit, the command is processed immediately; otherwise, it will wait its turn in the queue. Commands in this queue include file transfers and commands configured as Job actions. The default is 10.

hub.highpriorityevent.threads

High-priority commands are ones that need to run right away and are expected to have a quick response. These commands use a separate queue to help ensure that they are not backed up or put on hold behind long running commands such as file transfers and commands configured as Job actions. The commands that run through the high-priority queue include status queries to see if a job is still running, file listings to support the Gateway Administrator Browse actions, and file listings required by scans. The default is 10.

hub.responseevent.threads

The number of command responses to process in parallel. The default is 10.

hub.command-api.interface

The network interface used by Gateway Administrator to send commands to the Hub.

hub.command-api.port

The listening port on the Hub used by Gateway Administrator to send commands to the Hub. This value must match the value for [Hub listening port](#) configured on the [Edit Hub page](#).

restengine.ssl.keystore

The path to the keystore that contains the server certificate and private key. In most cases, you will not change these files on the Hub.

restengine.ssl.keystoretype

The file type of the keystore that contains the server certificate and private key. The only supported Java keystore type is BCFKS.

restengine.ssl.keystorepassword

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

hub.changedetection.waittime

In order to avoid processing files that are in use, the Hub uses directory listing comparisons to determine if files are currently changing. When a comparison of two listings shows no new files, no changes in file size, and no changes to file timestamps, the files are considered to be inactive. This setting specifies the time to wait (in seconds) between these directory listings. With a shorter wait time, Job actions happen sooner, but this also increases the chance of erroneously determining that a file is not being changed when it actually is. A longer wait time decreases those chances but also delays the job.

Reflection Gateway Data Files

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

- ♦ [Gateway Administrator \(page 121\)](#)
- ♦ [Reflection Hub \(page 122\)](#)
- ♦ [Reflection Transfer Server \(page 122\)](#)
- ♦ [Reflection for Secure IT Server for Windows and Reflection Secure Shell Proxy \(page 123\)](#)

Gateway Administrator

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

```
C:\Program Files\Micro Focus\ReflectionGateway\
```

| Files | Data description |
|--|--|
| <code>\GatewayAdministrator\conf\container.properties</code> | Gateway Administrator properties file (page 117) . |
| <code>\GatewayAdministrator\etc\database</code> | The default HyperSQL database. (Not used if you have configured an alternate database .) |

Files

\GatewayAdministrator\etc\

Data description

*.rnd - Queued events.

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

*.cer and *.bcfks - Gateway Administrator certificates and keystore files

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

Reflection Hub

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

C:\Program Files\Micro Focus\ReflectionGateway\

Files

\Hub\conf\container.properties

Data description

Hub [properties file \(page 120\)](#).

\Hub\etc\

*.cer and *.bcfks - Hub certificates and keystore files.

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

*.rnd - Queued events.

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

ga-response-service.properties - Automatically maintained file with information for connecting to Gateway Administrator. Do not modify this file manually.

trustedGA.cer - The certificate used to authenticate Gateway Administrator.

Reflection Transfer Server

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

C:\Program Files\Micro Focus\ReflectionGateway\

| Files | Data description |
|---|---|
| \TransferServer\conf\container.properties | Transfer Server properties file (page 119) . |
| \TransferServer\etc\ | Transfer Server certificates Do not delete any of the existing certificates or keystore files in these locations. The server certificates located here are required for communication between Reflection Gateway components. |

Reflection for Secure IT Server for Windows and Reflection Secure Shell Proxy

| Directory | Data description |
|---|--|
| C:\ProgramData\Micro Focus\RSecureServer\ | Reflection for Secure IT Server for Windows settings, server certificates, key files, and the credential cache |

Backing Up Gateway Administrator Data

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

C:\Program Files\Micro Focus\ReflectionGateway\GatewayAdministrator\

- ◆ \conf*.*
- ◆ \etc*.*
- ◆ If you have installed a commercial certificate, back up the appropriate .bcfks file, as specified in the [properties \(page 117\)](#) file using the **servletemine.ssl.keystore** setting.

Related Topics

- ◆ [“Ensuring High Availability of Reflection Gateway Services” on page 143](#)

Changing the Gateway Administrator Database

Gateway Administrator installs with a HyperSQL database, which is used by default to store Gateway Administrator data. This default database is suitable for initial testing. For configuring a high availability production environment, you will need to configure Gateway Administrator to use an external database running on a different system.

Install MySQL

- 1 Download and run the MySQL installer from the MySQL Downloads page:
<http://dev.mysql.com/downloads/installer/>
- 2 Run the installer on the system you want to store your database.
- 3 Make a note of the root password. You will need this to create the database.

Install the JDBC Driver for MySQL (Connector/J)

- 1 Download the driver from the MySQL downloads page:

<http://www.mysql.com/products/connector/>

- 2 On the system running Reflection Gateway Administrator service, navigate to GatewayAdministrator\lib folder. The default location is:
C:\Program Files\Micro Focus\ReflectionGateway\GatewayAdministrator\lib
- 3 Copy the driver jar file to this location (for example mysql-connector-java-5.1.44-bin.jar).

Create the database

Use the MySQL command line tool or MySQL WorkBench to create a database. For example, to create a database with the name "gateway" using the command line tool:

- 1 On the system running MySQL, start the command line client. For example:
Start > MySQL Server 5.7 > MySQL 5.7 Command Line Client
- 2 Enter the MySQL root password.
- 3 You'll see the following prompt:
mysql>
- 4 Create the database as shown here. (Note that a semicolon is required to complete the command.)
mysql> create database gateway;

Create the database user that Gateway Administrator will use to connect to the database

If MySQL is running on the same server as Gateway Administrator, you can use the MySQL root user without making any modifications to this user.

If the database is installed on a different system than Gateway Administrator, the user must be able to connect from a remote host using the host's network name or IP address. You can use MySQL Workbench or a command line to grant network access by allowing access from a specific host, or using the % wildcard to allow access from any host.

For example, to use the MySQL command line to create a user called gwuser with access to Gateway Administrator from any host:

- 1 On the system running MySQL, start the command line client.
- 2 Enter the following commands, replacing `some_password` with the actual password you want to use for this user.

```
CREATE USER 'gwuser'@'%' IDENTIFIED BY 'some_password';  
GRANT ALL PRIVILEGES ON gateway.* to 'gwuser'@'%';
```

- 3 Make a note of the username and password; you will need these to configure Gateway Administrator.

Configure Gateway Administrator to use the MySQL database

To configure Gateway Administrator to use the MySQL database, you will edit the [Gateway Administrator properties file](#). To do this you must be an Administrator on the Windows system running Gateway Administrator.

- 1 Open the Gateway Administrator properties file in a text editor. The default location is:
C:\Program Files\Micro Focus\ReflectionGateway\GatewayAdministrator\conf\container.properties
- 2 Comment out the HyperSQL settings, and uncomment the MySQL settings. Configure the MySQL hostname, database name, user name, and password. For example:

```
# HyperSQL (default)
#jdbc.url=jdbc:hsqldb:file:../etc/database/gateway.db
#jdbc.username=sa
#jdbc.password=
#hibernate.dialect=org.hibernate.dialect.HSQLDialect

# MySQL (recommended for production or clustered environments)
jdbc.url=jdbc:mysql://myhost:3306/gateway?useSSL=false
jdbc.username=gwuser
jdbc.password=some_password
hibernate.dialect=org.hibernate.dialect.MySQLDialect
```

- 3 [Restart the Reflection Gateway Administrator service \(page 140\)](#) and wait until the [server.log \(page 97\)](#) shows the message “Server container started.”
- 4 Log in to Gateway Administrator using the default user and password (`admin/secret`).
Any settings you configured using the default database will need to be redone using the new database.
- 5 If you have configured the Reflection Secure Shell Proxy to enable connections from Reflection Gateway users, repeat the Activate and Verify action. (See [“Enable Reflection Gateway Connections in the Reflection Secure Shell Proxy” on page 32.](#))

Job Administrative Topics

- ♦ [“Configure Preset Actions and Email Notifications using a Job Template” on page 125](#)
- ♦ [“How Reflection Gateway Determines if Files have Changed” on page 126](#)

Configure Preset Actions and Email Notifications using a Job Template

You can use a Job template to configure one or more preset actions that will always run before any actions configured by Gateway Administrator users. You can also use templates to provide preconfigured email notifications for Job success and failure notifications.

For example, you could create a template to transfer all files to a designated location, then screen these files for viruses. Any failure in this process will send a failure notification to an administrator whose email is configured in the template.

Actions that have been configured using a Job template are visible in the [New/Edit Job](#) page under [Preset Actions](#). (This section is visible only when a Job template is configured.) Gateway Administrator users can view the details of these actions, but cannot make changes.

Before you begin

- ♦ Have a Windows administrator account on the computer running the Reflection Gateway Administrator service.

Creating or editing a Job template requires write access to the files in the Reflection Gateway installation folder.

- ♦ Confirm that all servers required for your preset actions have been [added \(page 27\)](#) to Gateway Administrator.

The Reflection Gateway Administrator service will fail to start if a Job template is in place that uses servers that haven't been added.

- ◆ Test your Job actions using the Gateway Administrator [New/Edit Job](#) page.
This is not required, but is recommended. Any change you make to an action in a Job template requires a restart of the Reflection Gateway Administrator service before it can be tested.

To configure preset actions using a Job template

- 1 Navigate to Gateway Administrator `conf` folder. The default location is:
`C:\Program Files\Micro Focus\ReflectionGateway\GatewayAdministrator\conf`
- 2 Create a copy of `jobTemplate.xml.example` and open it in a text editor.
The template file is an XML file. The example file shows sample data for a Job that includes a transfer action followed by a command action.
- 3 Edit the file. You can delete elements you don't want to pre-configure, and edit or add elements as needed. For example:
 - ◆ In the `TransferAction` and `CommandAction` elements, change "targetServer" to your actual server name(s).

NOTE: The Reflection Gateway Administrator service will fail to start if `jobTemplate.xml` specifies invalid servers.

 - ◆ In the `CommandAction` element, replace the sample command.
 - ◆ Add or delete `TransferAction` and `CommandAction` elements as needed.
 - ◆ Enter correct email addresses for `SuccessAction` or `FailureAction`, or delete these elements. Setting these values in the template configures read-only values for the **To:** field in email notification messages. The **Cc:** field remains editable, so users creating Jobs can configure email notification to their own email address. If you delete the `SuccessAction` or `FailureAction` elements from the template, there will be no default failure and success notifications, and users will be able to configure all fields.
- 4 Save the file as `jobTemplate.xml` and put it in Gateway Administrator `conf` folder.
Restart the Reflection Gateway Administrator service and wait until the `server.log` ([page 97](#)) shows the message "Server container started."
- 5 Log in to Gateway Administrator and create a new Job to confirm your template settings:
 - ◆ If your template includes `TransferAction` or `CommandAction` elements, you'll see a **Preset Actions** section with that shows your template actions. These can be viewed but not edited.
 - ◆ If your template includes `SuccessAction` or `FailureAction`, all fields except the **Cc:** field will be preconfigured and read-only.

How Reflection Gateway Determines if Files have Changed

Job actions are triggered when files change in a scanned directory. To determine which files in a directory have changed, the Reflection Hub service compares directory listings of that directory. A file is marked as changed if any of these conditions are met:

- ◆ It is new in the second listing, which means the file was added to the directory between the two listings.
- ◆ The modification timestamp changed.
- ◆ The file size changed.

Transfer Site Administrative Topics

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

In this Section

- ♦ [“Change the Transfer Site Directory used by the Reflection Secure Shell Proxy” on page 127](#)
- ♦ [“Use an Added SFTP Server as the Transfer Site File Server” on page 128](#)
- ♦ [“Configure Connections to Remote SFTP Servers from the Reflection Secure Shell Proxy” on page 128](#)
- ♦ [“Customize the Look of the Transfer Client Web Pages” on page 130](#)
- ♦ [“Security Recommendations for the Reflection Secure Shell Proxy” on page 130](#)

Change the Transfer Site Directory used by the Reflection Secure Shell Proxy

The Transfer Site file server setting is configured in Gateway Administrator under **System > File Servers**. By default, Reflection Gateway creates Transfer Site directories on the Reflection Secure Shell Proxy running on the Reflection Gateway Proxy.

- ♦ The base directory on the Reflection Secure Shell Proxy is configured using the Reflection Secure Shell Proxy console, not using Gateway Administrator. This can be a local folder on the Reflection Secure Shell Proxy computer or an accessible network share.
- ♦ The name and location of the base directory you configure for your file server is not made visible to client users. The folder name that users see when they connect is the value you specify for **Transfer site name** when you create a Transfer Site. The actual subdirectory on the file server is the value you specify for **Directory name**, which can be the same or different.

The default base directory on the Reflection Secure Shell Proxy is:

```
C:\ProgramData\Micro Focus\RSecureServer\Reflection\
```

To modify the base directory on the Reflection Secure Shell Proxy

- 1 Start the Reflection Secure Shell Proxy console. It is installed in the Windows Start menu (or Apps list) under **Micro Focus Reflection for Secure IT Gateway > Reflection Secure Shell Proxy**.
- 2 On the **Reflection Gateway Users** pane, edit **Reflection base path**.

NOTE: You can specify a local path, a mapped drive, or a UNC path. If you specify a network location, set **Micro Focus Reflection Gateway Administrator user access account** to a user who has access to that location.

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

Related Topics

- ♦ [“Use an Added SFTP Server as the Transfer Site File Server” on page 128](#)

Use an Added SFTP Server as the Transfer Site File Server

Use the following procedure to designate an added SFTP for Transfer Site file exchange. Typically this will be a server running in your internal network. This is the recommended configuration when the Reflection for Secure IT Gateway is running in the DMZ. With this configuration, data streams continuously through the proxy, eliminating the need to save files on this server. Data passed to the SFTP server is securely encrypted.

Before you begin

- ◆ [Add the SFTP server to the list of available servers using System > File Servers \(page 27\)](#). Set the base directory for this server to the directory you want to use for Transfer Site file exchange.

NOTE: The name and location of the base directory you configure for your server is not made visible to client users. The folder name that users see when they connect is the value you specify for **Transfer site name** when you create a Transfer Site. The actual subdirectory on the file server is the value you specify for **Directory name**, which can be the same or different.

To designate an added SFTP server as the Transfer Site file server

- 1 Log on to Gateway Administrator using an account in the Administrators group (or any account that has the **System setup** role enabled).
- 2 Go to **System > File Servers**.
- 3 Use the **Transfer site file server** drop-down list to select the added SFTP server.
- 4 Click **Save**.

Related Topics

- ◆ [“File Servers Tab” on page 90](#)

Configure Connections to Remote SFTP Servers from the Reflection Secure Shell Proxy

The File **Transfer site file server** setting in Gateway Administrator allows you to specify a single SFTP server for Transfer Site file exchange. Any Transfer Site you define using Gateway Administrator uses a directory on this server or a network location available to this server using a UNC path. This option is easy to use and configure, and is the recommended configuration.

It is also possible to configure directory access on additional servers using the **SFTP Directories** feature of the **Reflection Secure Shell Proxy**; however, directories made available this way are managed differently from Transfer Sites. Review the following limits and differences before you proceed.

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

Direct users to connect directly to the Reflection Secure Shell Proxy using an [alternate SFTP client](#), instead of using the Reflection Transfer Client.

-OR-

Ensure that all users have at least one Transfer Site configured in Gateway Administrator.

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

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

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

- 1 Start the Reflection Secure Shell Proxy console. It is installed in the Windows Start menu (or Apps list) under **Micro Focus Reflection for Secure IT Gateway > Reflection Secure Shell Proxy**.
- 2 From the **Configuration** tab, click **SFTP Directories** in the left panel, then click **Add**. This opens the **Accessible Directory Settings** dialog box.
- 3 Enter a **Virtual directory** name. This is the folder name that will be visible to users.
- 4 Select **Remote SFTP server**. This opens the **Remote SFTP Server Connection** dialog box.
 - ◆ For **Host**, specify the name or IP address of the SFTP server.
 - ◆ Click **Retrieve** to retrieve the public key used to authenticate this server.
 - ◆ For **Remote SFTP username** and **Password**, enter the credentials of the user account that will provide access to the file system on the remote SFTP server.
 - ◆ Under **Remote base directory**, click **Browse** to select the directory you want to make available to users. This must be a directory accessible to the user you entered for **Remote SFTP username**.
- 5 Click **Test Connection**. You should see a message saying that the connection was successful.
- 6 Click **OK** to close the dialog boxes and return to the **SFTP Directories** pane.

NOTE: The **User login directory** option, including the default /Home directory, is not used for Reflection Gateway users.

- 7 Save your settings (**File > Save Settings**).

Use the next procedure to limit access to a directory on an SFTP server to members of a Reflection Gateway group or to an individual Reflection Gateway user.

To configure directory access for a Reflection Gateway group or user

- 1 From the Reflection Secure Shell Proxy console **Configuration** tab, under **Subconfiguration** click either **User Configuration** or **Group Configuration**.
- 2 Click **Add**.
- 3 Click **Domain** (for user configuration) or set **Group type** to **Domain** (for group configuration).
 - ◆ For members of the ReflectionGateway LDAP server, set the domain name to `ReflectionGateway`.
 - ◆ For members of an added LDAP server, use the **Domain name** as it appears on the **LDAP Servers** page in Gateway Administrator.
- 4 Enter the name of the user or group your are configuring.
- 5 In the left portion of the **Group Configuration** dialog box, click **SFTP Directories**.
- 6 Clear the **Inherit directories** check box.
- 7 Click **Add** to open the **Accessible Directory Settings** dialog box.

- 8 Configure the remote directory that will be available to this user or group, as described in the preceding procedure, starting with step 3.
- 9 Save your settings (**File > Save Settings**).

Customize the Look of the Transfer Client Web Pages

By default, the Transfer Client uses Micro Focus Reflection Gateway names and images. You can modify these web pages so that Transfer Client users see a page title and the images that identify your organization.

To customize the Transfer Client web pages

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

```
<install path>\TransferServer\services\webxfer-ui\webapps\custom
```

NOTE: Making changes in this location ensures that your modifications remain in place after a server restart or application upgrade. Changes made in other locations, or to the existing files, are not guaranteed to remain in place.

- 2 Locate the `custom-example` directory in `webapps` and copy the contents of this folder into your `custom` folder.
- 3 Edit `title.html`, replacing the sample title "Custom File Transfer" with the page title you want displayed in the user's browser.
- 4 View the contents of `branding.css`. This file configures images and related colors. Edit the styles to suit your design, create appropriate images as defined in this file, and replace the sample images with your custom images.
- 5 Start the Transfer Client or refresh the browser display to view the changes.

Security Recommendations for the Reflection Secure Shell Proxy

Use the following precautions to help ensure security on the Reflection Gateway Proxy (the system running the Reflection Secure Shell Proxy and the Reflection 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 Secure Shell Proxy console:
 - ◆ On the **Reflection Gateway Users** pane, leave **Allow server access to Reflection Gateway users only** and **Restrict Reflection Gateway users to file transfer sessions** selected. These default settings help minimize external user access to your system.
 - ◆ Change the user access account to an account with more limited privileges than the default service account.
 - ◆ Disable port forwarding for all users. To do this, clear both port forwarding options on the **Permissions** pane under **Tunneling**.
- ◆ [Configure firewalls \(page 21\)](#) that limit access to ports on your servers.

Server Certificate Management

When users log on to Gateway Administrator or the Reflection Transfer Client, the connection is made using HTTPS and the browser requires server authentication. By default, the Reflection Gateway servers send a self-signed security certificate to the browser for this purpose. (A self-signed certificate is signed by the same entity that it certifies.) The browser checks the digital signature in this certificate against its list of trusted [Certificate Authorities \(CAs\) \(page 153\)](#). With the default certificates, you see a certificate warning, because the signer of the certificate is not in your browser's list of trusted CAs.

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

- ♦ [“Replace the Default Server Certificate” on page 131](#)
- ♦ [“Configure Your Browser to Trust a Self-Signed Certificate” on page 134](#)
- ♦ [“Migrate PKCS#12 or JCEKS keystores to BCFKS keystores” on page 135](#)
- ♦ [“Using the Keytool Utility to Manage Keystores” on page 136](#)

Related Topics

- ♦ [“Configure Server Certificates” on page 34](#)

Replace the Default Server Certificate

To be able to start the Transfer Client and Gateway Administrator without seeing certificate warning messages, you can replace each of these self-signed certificates with a certificate from a well-known Certificate Authority (CA).

To replace self-signed certificates create a PKCS#12, or JKS keystore and migrate the file (.p12, .pfx, or .jks) to BCKFS. Server certificates must be stored in a FIPS compliant BCFKS keystore. Refer to the following procedures for details.

[Install a Server Certificate in a PKCS#12 File \(page 131\)](#)

[Install a Server Certificate in a Java Keystore \(page 133\)](#)

Install a New Server Certificate: PKCS#12 File

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

Before you begin

Obtain a [PKCS#12 \(page 153\)](#) file (*.p12 or *.pfx) that includes your private key and a certificate signed by a [Certificate Authority \(CA\) \(page 153\)](#).

NOTE

- ♦ The certificates that authenticate Reflection Gateway servers must use FIPS-compliant cryptography. You should request a FIPS-compliant certificate from your Certificate Authority. DSA keys used in the certificate must be either 1024, 2048, or 3072 bits. RSA keys must be either 2048 or 3072 bits.

- ♦ The PKCS#12 store must also use FIPS-compliant cryptography. If you have a PKCS#12 package that contains a FIPS-compliant private key, but the store encryption is not FIPS-compliant, the server will fail to start. To resolve this, you can [re-encrypt the PKCS#12 file \(page 135\)](#) or [import the file into a Java keystore \(page 139\)](#).
 - ♦ The PKCS#12 store and the private key must be protected with the same password.
-

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

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

```
<install path>\TransferServer\etc\  
<install path>\GatewayAdministrator\etc\  

```

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

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

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

```

- 3 Open `container.properties` in a text editor. (You must be a Windows administrator to be able to edit this file.) Remove the comment character (#) from the following lines. Edit these lines to specify a PKCS12 package and enter your certificate name and password. For example:

```
servletengine.ssl.keystore=../etc/myserver_cert.p12  
servletengine.ssl.keystoretype=PKCS12  
servletengine.ssl.keystorepassword=myspassword  

```

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

- 4 Restart the server you are configuring. See [“Start and Stop the Reflection Transfer Server” on page 140](#) and [“Start and Stop the Reflection Gateway Administrator Service” on page 140](#).
- 5 If you replaced the Gateway Administrator certificate after using the default certificate, you will need to update server authentication configuration:
 - ♦ From the Reflection Secure Shell Proxy console, repeat the [Activate and verify \(page 32\)](#) action.
 - ♦ [Reset the server authentication certificate \(page 141\)](#) on any hubs that have been added, then reactivate those hubs from Gateway Administrator.
- 6 Confirm that you can log on to the Transfer Client or Gateway Administrator.

If you can't log in, or if you continue to see a certificate warning message, see [Troubleshooting Server Certificate Setup \(page 109\)](#).

Related Topics

- ♦ [“Server Certificate Management” on page 131](#)
-

NOTE: If you are using a load-balancing proxy to ensure high availability of Reflection Gateway services, you will need to configure duplicate server systems after making these changes. For details, see [“Ensuring High Availability of Reflection Gateway Services” on page 143](#),

Install a New Server Certificate: Java Keystore

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

Before you begin

Obtain a “Java keystore” on page 153 (*.bcfks) file that contains your private key and a certificate signed by a Certificate Authority (CA) (page 153). You can use the following procedures to create your keystore using the Java **keytool** utility.

- ♦ “Generate a Key Pair and Create a Keystore” on page 136.

NOTE: DSA keys must be either 1024, 2048, or 3072 bits. RSA keys must be either 2048 or 3072 bits.

- ♦ Create a Certificate Signing Request and submit it to a CA (page 137).
- ♦ Import the CA-signed certificate into your keystore (page 138).

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

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

```
<install path>\TransferServer\etc\  
<install path>\GatewayAdministrator\etc\  

```

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

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

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

```

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

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

```

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

- 4 Run the new `migrate_keystore.bat` file.
- 5 Open `container.properties` in a text editor and edit the following lines:

```
servletengine.ssl.keystore=../etc/migrated.bcfks  
servletengine.ssl.keystoretype=BCFKS  

```

- 6 Restart the server you are configuring. See “Start and Stop the Reflection Transfer Server” on page 140 and “Start and Stop the Reflection Gateway Administrator Service” on page 140.

- 7 If you replaced the Gateway Administrator certificate, you must repeat the **Activate and verify** (page 32) action on the Reflection Secure Shell Proxy. This reestablishes the connection to the Gateway Administrator using the new certificate.
- 8 Confirm that you can log on to the Transfer Client or Gateway Administrator. If you can't log in, or if you continue to see a certificate warning message, see [Troubleshooting Server Certificate Setup](#) (page 109).

NOTE: If you are using a load-balancing proxy to ensure high availability of Reflection Gateway services, you will need to configure duplicate server systems after making these changes. For details, see [“Ensuring High Availability of Reflection Gateway Services”](#) on page 143,

Configure Your Browser to Trust a Self-Signed Certificate

If you use the default Reflection Gateway certificates, you will see a certificate warning when you connect to the Gateway Administrator and the Transfer Client. You can use the following procedures to remove these warnings without modifying the server certificates.

NOTE: The procedures below are appropriate for testing. They may also be appropriate if only a small number of users access Gateway Administrator. However, before you deploy the Transfer Client to end users, or provide administrative access to a larger number of users, you should configure Reflection Gateway to use certificates signed by a well-known Certificate Authority. (See [“Replace the Default Server Certificate”](#) on page 131.) With the updated certificates in place, the following procedures are not necessary.

To add an untrusted certificate to the Internet Explorer trusted root store

- 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.
- 3 In the Certificate Error message, 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 exception for an untrusted certificate in Firefox

- 1 When you see a warning that the connection is untrusted, click **Advanced**.
- 2 Click **Add Exception**.
- 3 Leave **Permanently store this exception** selected and click **Confirm Security Exception**.

To add an untrusted certificate to the trusted root store from Chrome

NOTE: Chrome is supported for connections to Gateway Administrator, but not for transfers using the Reflection Transfer Client.

- 1 When you see a message saying your connection is not private, click **Advanced**, then click the **Proceed to** link log in.
- 2 Save the presented certificate to a file. To do this:
 - ♦ Click the View site information icon (a padlock) in the address bar: 
 - ♦ Click **Certificate Information**.
 - ♦ On the **Details** tab, click **Copy to File** and save the file using defaults.
- 3 Locate and double-click the certificate file you just saved.
- 4 On the certificate **General** tab, click **Install 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.

Migrate PKCS#12 or JCEKS keystores to BCFKS keystores

You can use an installed script called `migrated_keystore.bat` to convert your PKCS#12 or JCEKS keystores to BCFKS keystores.

This script examines the `container.properties` to find custom keystores that have been added and automatically converts them to BCFKS.

IMPORTANT: You need to know the password that protects this file.

Before you begin

- 1 Open a command window.
- 2 Run the following two commands to place Java in the default path:

```
set JAVA_HOME="c:\Program Files\Common Files\Micro Focus\ServerJDK\1.8.0_151"  
set PATH=%JAVA_HOME%\bin;%PATH%
```

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

- 1 On the computer running the Reflection Transfer Server, open a command window running as an administrator.
- 2 Navigate to `TransferServer\bin` in the Reflection Gateway installation folder. The default location is:

```
C:\Program Files\Micro Focus\ReflectionGateway\Gateway\TransferServer\bin
```

- 3 Run the `migrated_keystore.bat` batch file.
- 4 Modify the `container.properties` and update the following settings:

```
servletengine.ssl.keystore=..\etc\migrated.bcfks  
servletengine.ssl.keystoretype=BCFKS
```

NOTE: If these passwords don't match, the server will not be able to use the keystore.

Using the Keytool Utility to Manage Keystores

The Java **keytool** utility is a command-line tool that can be used to manage keys and certificates. Depending on how you obtain certificates, you can use one or more of these procedures to manage your Reflection Gateway certificates. For more complete documentation, refer to the **keytool** documentation (<https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html>).

In this Section

- ♦ “Run the Keytool Utility” on page 136
- ♦ “Generate a Key Pair and Create a Keystore” on page 136
- ♦ “Create and Submit a Certificate Signing Request” on page 137
- ♦ “Import Certificates from a p7b package into your Java Keystore” on page 138
- ♦ “Import Individual Certificates into your Keystore” on page 138
- ♦ “Import a PKCS#12 File into a Java Keystore” on page 139

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.
- 2 Navigate to the folder that contains `keytool.exe` or add this folder to your path. (Confirm the actual Server JDK version for your installation.) For example:

```
SET PATH=%PATH%;C:\Program Files\Common Files\Micro  
Focus\ServerJDK\<version>\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 136) utility to generate a key and save it to a Java keystore.

NOTE

- ♦ The CA you use might have specific options required for creating an HTTPS certificate. Review the instructions provided by the CA before creating your key pair.
 - ♦ DSA keys used in Reflection Gateway server certificates must be 1024, 2048, or 3072 bits. RSA keys must be either 2048 or 3072 bits.
-

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.bckfs` in this example). The example shown here prompts you to enter values for items that make up the distinguished name (DN) in the certificate. See the example below to enter these values directly on the command line.


```
keytool -genkeypair -providertype BCFIPS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath ../bc-
fips-1.0.1.jar -alias rgateway -keyalg RSA -keysize 2048 -keystore
newkeystore.bcfks -validity 365 -storetype BCFKS -storepass "<password>"
```

- 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 Gateway server (for example `gateway.mycompany.com`). This value is used as the CN (Common Name) in the certificate. If the CN in a certificate doesn't match the actual DNS name used to access the server, you will see a certificate warning when you connect to the server.
 - ◆ When you are prompted with "What is the two-letter country code for this unit?"

You must enter a valid two-letter country code (for example `US`).
- 3 When you are prompted for a password for the alias, press Enter to use the same password you used for the keystore.

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

```
keytool -genkeypair -providertype BCFIPS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath ../bc-
fips-1.0.1.jar -dname "CN=gateway.mycompany.com, O=My Company, C=US" -alias
rgateway -keyalg RSA -keysize 2048 -keystore newkeystore.bcfks -validity 365 -
storetype BCFKS.
```

Create and Submit a Certificate Signing Request

This procedure uses the Java [keytool \(page 136\)](#) 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 \(page 136\)](#).

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 gateway -providertype BCFIPS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath ../bc-
fips-1.0.1.jar -keystore newkeystore.bcfks -file cert_request.csr -ext
ExtendedkeyUsage=serverAuth -storetype BCFKS
```

- 2 Enter your keystore password when prompted.
- 3 You will see a message saying that the certificate request has been saved to the file you specified (`cert_request.csr` in this example).
- 4 Submit this CSR to your CA. You will need the contents of the CSR file. Open the file in a text editor. The contents should include a header and footer with encoded data between them. When you submit the request, copy the entire file, including the `BEGIN` and `END` lines.

```
-----BEGIN CERTIFICATE REQUEST-----
```

<encoded data>

-----END CERTIFICATE REQUEST-----

Import Certificates from a p7b package into your Java Keystore

The Certification Authority may provide you with a PKCS#7 package (*.p7b) that contains the full chain of certificates required to authenticate your server (the CA-signed server certificate, intermediate certificates, and the CA root certificate). This procedure uses Java [keytool \(page 136\)](#) command to import the certificates from the p7b file into your Java keystore.

NOTE: If you have individual certificates not contained within a p7b package do not use this procedure. You will need to import each certificate separately. See the procedure described in [“Import Individual Certificates into your Keystore” on page 138.](#)

Before you begin

- ◆ Obtain a PKCS#7 package (*.p7b) from the Certification Authority that contains the CA-signed server certificate, intermediate certificates, and the CA root certificate.
- ◆ You need to know the keystore name, password, and alias you used when you [created the keystore \(page 136\)](#).

To import certificates contained within a p7b file

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

```
keytool -importcert -alias rgateway -trustcacerts -file FullChainOfCerts.p7b -
providername BCFIPS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath ../bc-
fips-1.0.1.jar -keystore newkeystore.bcfks -storetype BCFKS
```

Import Individual Certificates into your Keystore

Use this procedure if certificates (the CA-signed server certificate, intermediate certificates, and the CA root certificate) are obtained as individual certificates instead of in a single PKCS#7 (*.p7b) file. This procedure uses a series of Java [keytool \(page 136\)](#) commands to import these certificates into an existing keystore. Use the order of import as shown in the procedure: import the root CA first, then any required intermediate certificates, and finally, the CA-signed server certificate.

NOTE: If your certificate was provided within a p7b package, you do not need to import each certificate separately. Instead, use the procedure described in [“Import Certificates from a p7b package into your Java Keystore” on page 138.](#)

Before you begin

- ◆ Obtain a server certificate for your server signed by a Certificate Authority.
- ◆ Obtain the trusted root CA certificate for the Certificate Authority and any required intermediate certificates.
- ◆ You need to know the keystore name, password, and alias you used when you [created the keystore \(page 136\)](#).

To import certificates into your Java keystore

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

```
keytool -importcert -alias root -file CAcert.cer -providertype BCFIPS -  
providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -  
providerpath ../bc-fips-1.0.1.jar -keystore newkeystore.bcfks -storetype  
BCFKS.
```

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

```
keytool -importcert -alias intermediate -trustcacerts -file  
IntermediateCAcert.cer -providertype BCFIPS -providerclass  
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath ../bc-  
fips-1.0.1.jar -keystore newkeystore.bcfks -storetype BCFKS
```

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

```
keytool -importcert -alias rgateway -trustcacerts -file EndEntitycert.cer -  
providertype BCFIPS -providerclass  
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath ../bc-  
fips-1.0.1.jar -keystore newkeystore.bcfks -storetype BCFKS
```

Import a PKCS#12 File into a Java Keystore

This procedure uses the Java [keytool](#) (page 136) utility to create a Java keystore from a PKCS#12 file.

Before you begin

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

To import a PKCS#12 file into a Java keystore

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

```
keytool -importkeystore -v -srckeystore cert_file.p12 -srcstoretype PKCS12 -  
providertype BCFIPS -providerclass  
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath ../bc-  
fips-1.0.1.jar -destkeystore newkeystore.bcfks -deststoretype BCFKS.
```

NOTE: The keystore type you specify for `deststoretype` must match the type specified for `servletengine.ssl.keystore.type` in the server's `container.properties` file. BCFKS 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.

Managing the Reflection Gateway Services

In this Section

- ♦ “Start and Stop the Reflection Gateway Administrator Service” on page 140
- ♦ “Start and Stop the Reflection Transfer Server” on page 140
- ♦ “Start and Stop the Reflection Hub” on page 141
- ♦ “Reset Server Authentication on a Reflection Hub” on page 141
- ♦ “Start and Stop the Reflection Secure Shell Proxy” on page 141
- ♦ “Reset Gateway Administrator to All Defaults” on page 142

Start and Stop the Reflection Gateway Administrator Service

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

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

- 1 On the Gateway Administrator computer, open the Windows Services console.
- 2 Select the service called "Micro Focus Reflection Gateway Administrator" and click start, stop, or restart.

NOTE: After the service has started, Gateway Administrator is not immediately available. To confirm that service startup is complete, look for the message “Server Container started” in the Gateway Administrator [server.log](#) (page 97).

Start and Stop the Reflection Transfer Server

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

To start or stop the Reflection Transfer Server service

- 1 On the Reflection Gateway Proxy computer, open the Windows Services console.
- 2 Select the service called "Micro Focus Reflection Transfer Server" and click start, stop, or restart.

NOTE: After the service has started, the Reflection Transfer Client might not be immediately accessible. If you cannot start the Transfer Client, wait a minute or two and try again

Start and Stop the Reflection Hub

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

To start or stop the Reflection Hub service using the Windows Services Console

- 1 On the Gateway Administrator computer, open the Windows Services console.
- 2 Select the service called "Micro Focus Reflection Hub" and click start, stop, or restart.

Reset Server Authentication on a Reflection Hub

When you activate a Hub, Gateway Administrator and the Hub exchange certificates. These certificates are used for server authentication in subsequent connections. If you reconfigure your systems (for example connecting to a Hub from a different instance of Gateway Administrator, or changing from the default self-signed Gateway Administrator certificate to a CA-signed certificate), server authentication must be reconfigured.

The following symptoms may indicate that the Hub and Gateway Administrator authentication is failing.

- ♦ A Job fails with an entry in the Gateway Administrator log that includes: "SSLErrorException invoking https://<hub_server>:9188."
- ♦ In the Gateway Administrator user interface, you see a message saying, "Failed to activate the hub." when you click **Save and Activate** in the **New/Edit Hub** page and you have confirmed that the server name and port are correct.

To resolve this problem, you can reset the Hub.

To reset the certificate used by the Hub to authenticate the Gateway Administrator server

- 1 As an administrator of the computer running the Reflection Hub service, navigate to `Hub\bin` in the Reflection Gateway installation folder. The default location is:

```
C:\Program Files\Micro Focus\ReflectionGateway\Hub\bin
```
- 2 Run the `resetserver.bat` file.
You will see a prompt asking if you want to reset the Hub to its initial state.
- 3 Press `y`.
The script stops the service, removes the saved Gateway Administrator server certificate, then restarts the service.
- 4 Log on to Gateway Administrator using an account that has the **System setup** role enabled.
- 5 Go to **System > Hubs**, select the Hub you reset, and click **Edit**. On the **Edit Hub** page, click **Save and Activate**.

Start and Stop the Reflection Secure Shell Proxy

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

To use the Reflection Secure Shell Proxy console

- 1 Start the Reflection Secure Shell Proxy console. It is installed in the Windows Start menu (or Apps list) under **Micro Focus Reflection for Secure IT Gateway > Reflection Secure Shell Proxy**.
- 2 Use the **Action** menu items or the toolbar buttons to start and stop the server.

To use the Windows Services console

- 1 On the Reflection Gateway Proxy computer, open the Windows Services console.
- 2 Select the service called "Micro Focus Reflection Secure Shell Proxy" and click start, stop, or restart.

Reset Gateway Administrator to All Defaults

Gateway Administrator installs a reset batch file that resets the Gateway Administrator to the original shipping state. If you are using the default HyperSQL database, running this batch file has the following effects:

- ◆ Deletes all users and groups you have added to the ReflectionGateway user list. The default "admin" account, Administrators group, and File Transfer Administrators group will be recreated when you restart the server.
- ◆ Deletes all Transfer Sites and Jobs.
- ◆ Deletes all Post Transfer Actions.
- ◆ Restores all System settings to the original defaults.
- ◆ Deletes any queued actions and emails.

If you have [changed the database \(page 123\)](#), this script does not affect your Gateway Administrator data. It's only affect in this case is to delete queued actions and emails.

CAUTION: If you are using the default HyperSQL database, resetting the Gateway Administrator removes all saved users, Transfer Sites, and system settings. Use this option only to clear the data during initial testing, or if you cannot access the server with any available credentials and understand that all existing data and customizations will be lost.

To reset the Gateway Administrator to factory defaults

- 1 On the Gateway Administrator computer, open a command window running as an Administrator.
- 2 As an administrator of the computer running the Reflection Gateway service, navigate to `GatewayAdministrator\bin` in the Reflection Gateway installation folder. The default location is:

```
C:\Program Files\Micro Focus\ReflectionGateway\GatewayAdministrator\bin
```
- 3 Run the `resetserver.bat` file.
You will see a prompt asking if you want to reset the Gateway Administrator to its initial state.
- 4 Press `Y`.
Without any further confirmation, the script stops the service, removes all saved user data and system settings, then restarts the service.
- 5 Wait until the [server.log \(page 97\)](#) shows the message "Server container started," then connect to the Gateway Administrator and log in using "admin" and "secret".

Ensuring High Availability of Reflection Gateway Services

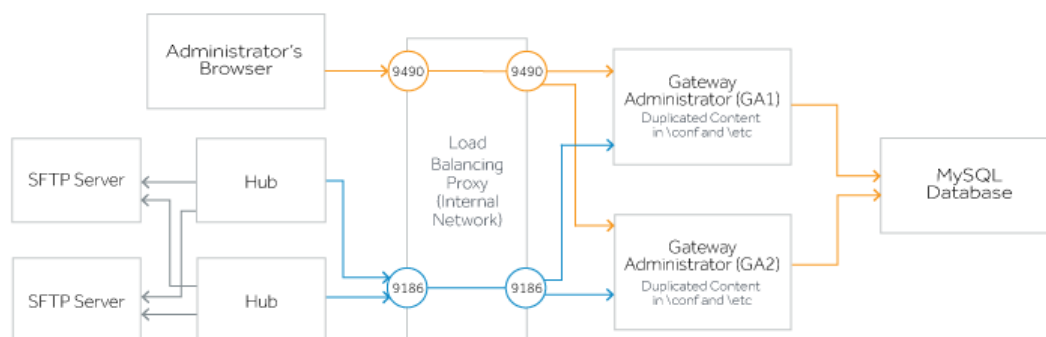
To ensure high availability of Reflection Gateway services, you can configure duplicate server systems and use a load-balancing proxy to manage connections between the components.

To support any load-balancing system for Reflection Gateway, you will need to create a database on a remote system and configure duplicate Gateway Administrator servers to communicate with this database. Details are provided in the procedures that follow. The database server should be configured for failover, for example using a Windows cluster. Failover configuration procedures for the database are not covered in this guide.

NOTE: The port values shown in these diagrams and in the [sample HAProxy configurations](#) are the defaults. The diagrams also omit some connections that do not need to be handled by the proxy. For more detailed information, see [“Ports and Firewall Configuration” on page 21](#).

Configuring high availability for Jobs

To support load balancing for jobs, you will need to create identically configured Gateway Administrator servers and use a load balancing proxy to manage connections to these servers, as shown here:

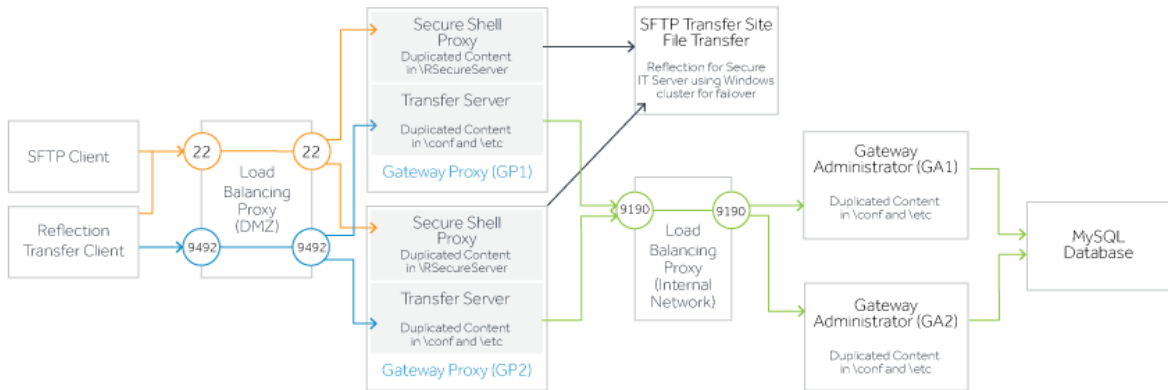


To set up load balancing for Jobs

- 1 Create identically configured Gateway Administrator systems that connect to the same database (page 145).
- 2 Configure a load balancing proxy to forward requests coming from administrators' browsers (port 9490) and Reflection Hub servers (port 9186) to the Gateway Administrator servers. For an example using HAProxy, see [“Sample Proxy configuration in the internal network” on page 149](#).
- 3 Install the Reflection Hub service on two or more systems and configure any Gateway Administrator instance to connect to each Hub.
 - ♦ On the **Hubs** tab, confirm that the Gateway Administrator server value for each Hub is specified using the network name or IP address that is configured on the load balancing proxy for connections from your Hub systems.
 - ♦ You can add or delete Hubs at any time after you have configured your database connection. The round robin connection to the Hubs is managed by Gateway Administrator and all Hub connection settings are stored in the common database. Increasing the number of hubs may improve performance if your jobs manage large numbers of file multiple transfers.

Configuring load balancing for Transfer Sites

Load balancing for Transfer Sites typically involves two load-balancing proxies—one in the DMZ and one in the internal network. The proxy in the DMZ forwards requests from transfer clients to identically configured Reflection Gateway Proxy systems. The proxy in the internal network forwards requests from the Reflection Gateway Proxy systems to identically configured Gateway Administrator systems.



To set up load balancing for Transfer Sites

- 1 Create identically configured Gateway Administrator systems that connect to the same database (page 145).
- 2 Create identically configured Reflection Gateway Proxy systems (page 147).
- 3 Configure a load balancing proxy in the DMZ to forward requests coming from Transfer Site users (ports 22 and 9492) to the services running on the Reflection Gateway Proxy systems. For an example using HAProxy, see “Sample Proxy configuration in the DMZ” on page 150.
- 4 Configure a load balancing proxy in the internal network to forward requests coming from the Reflection Gateway Proxy servers (port 9190) and from Administrator browsers (9490—not shown in the second diagram) to the Gateway Administrator systems. For an example using HAProxy, see “Sample Proxy configuration in the internal network” on page 149.
- 5 Configure a failover system for the Transfer Site file server. If the server is a Reflection for Secure IT Server for Windows, you can use a Windows cluster. See “Using a Server Cluster” in the Reflection for Secure IT Server Help.

Configuring load balancing for both Jobs and Transfer Sites

Setting up load balancing for both Jobs and Transfer Sites combines the procedures above.

To set up load balancing for both Jobs and Transfer Sites

- 1 Create identically configured Gateway Administrator systems that connect to the same database (page 145).
- 2 Create identically configured Reflection Gateway Proxy systems (page 147).
- 3 Configure a load balancing proxy in the DMZ to forward requests coming from Transfer Site users (ports 22 and 9492) to the services running on the Reflection Gateway Proxy systems. For an example using HAProxy, see “Sample Proxy configuration in the DMZ” on page 150.

- 4 Configure a load balancing proxy in the internal network. To support both Jobs and Transfer sites you will need to forward requests coming to Gateway Administrator from administrators' browsers (port 9490), Reflection Hub servers (port 9186), and the Reflection Gateway Proxy systems (port 9190). Examples for all of these are included in [“Sample Proxy configuration in the internal network” on page 149](#).
- 5 Install the Reflection Hub service on two or more systems and configure any Gateway Administrator instance to connect to each Hub.
 - ◆ On the **Hubs** tab, confirm that the Gateway Administrator server value for each Hub is specified using the network name or IP address that is configured on the load balancing proxy for connections from your Hub systems.
 - ◆ You can add or delete Hubs at any time after you have configured your database connection. The round robin connection to the Hubs is managed by Gateway Administrator and all Hub connection settings are stored in the common database. Increasing the number of hubs may improve performance if your jobs manage large numbers of file multiple transfers.
- 6 Configure a failover system for the Transfer Site file server. If the server is a Reflection for Secure IT Server for Windows, you can use a Windows cluster. See [“Using a Server Cluster”](#) in the Reflection for Secure IT Server Help.

Configure Duplicate Gateway Administrator Systems

To support high availability, you will configure and test an initial instance of Gateway Administrator, then create an identically-configured Gateway Administrator system and use a load-balancing proxy to distribute the load between these systems. Each Gateway Administrator system must:

- ◆ Use a common database.
- ◆ Use identical server certificates.
- ◆ Use identical copies of the Gateway Administrator properties file (`container.properties`).
- ◆ Use identical Job templates (if this optional feature is configured).

NOTE: Configuring more than two Gateway Administrator systems will not improve performance and may lead to slower response rates.

Before you begin

- ◆ Run the [Setup program](#) on each system that will run Gateway Administrator. Use the **Features** tab to install the Reflection Gateway Administrator feature. Restart Windows on each system. This starts the service and creates initial default settings files.
- ◆ Select one of the Gateway Administrator systems for initial configuration and testing. After you have this instance working, you will copy required files to duplicate the configuration on your second system.

Configure an initial Gateway Administrator system

- 1 [Configure Gateway Administrator to use an external database](#). The database should be located on a different system from each of the systems that will run Gateway Administrator. (This database should be configured for failover, for example using a Microsoft cluster. This procedure is not included here.)

- 2 If you are using a CA-signed certificate for server HTTPS authentication, replace the default self-signed server certificate with the CA certificate and test connections using the new certificate. See [“Replace the Default Server Certificate” on page 131](#). This certificate should be configured to authenticate the server name that will be used for connecting to your load-balancing proxy.
- 3 If you are using Transfer Site email notifications, [configure the URL that will be used to create links in email messages \(page 31\)](#). This requires an edit to the `container.properties` file.
- 4 If you are using [Job templates \(page 125\)](#), configure and test a `jobTemplate.xml` file.
- 5 Log onto Gateway Administrator and test your configuration.

Copy required files to the duplicate Gateway Administrator system

- 1 Locate the Gateway Administrator folder on your initial system. The default location is:

`C:\Program Files\Micro Focus\ReflectionGateway\GatewayAdministrator\`

- 2 Copy the following files to the duplicate system.

| Files | Details |
|--|--|
| <code>container.properties</code> | In the <code>conf</code> subfolder. Includes settings and password for connecting to the database. If configured, it includes the URL used in email notifications, and settings for using a CA-signed certificate. |
| <code>server.cer</code> | In the <code>etc</code> subfolder. |
| <code>server.bcfks</code> | A private key stored in <code>server.bcfks</code> is used to encrypt passwords for LDAP servers, SFTP servers, and SMTP servers. An identical private key must be present in each system to enable each server to encrypt or decrypt these passwords. |
| <code>servletcontainer.cer</code> <code>servletcontainer.bcfks</code> | These files contain the certificate and private key used to authenticate the server when users make HTTPS connections to Gateway Administrator. <ul style="list-style-type: none"> ◆ If you are using the default self-signed certificate, copy <code>servletcontainer.cer</code> and <code>servletcontainer.bcfks</code> located in the <code>etc</code> subfolder. ◆ If you are using a CA-signed certificate, find the certificate package file in the location specified in the <code>container.properties</code> file. For example: <code>servletengine.ssl.keystore=../etc/myCAkeystore.bcfks</code> Copy this file to the same location on each of the other systems. |
| <code>jobTemplate.xml</code> | In the <code>conf</code> subfolder. This file is only needed if you have configured a Job template. |

Related Topics

- ◆ [“Ensuring High Availability of Reflection Gateway Services” on page 143](#)

Configure Duplicate Reflection Gateway Proxy Systems

The Reflection Gateway Proxy system is required to support Transfer Sites. Two services run on this system:

- ♦ Reflection Transfer Server
- ♦ Reflection Secure Shell Proxy.

To support high availability, you will configure and test an initial instance of the Reflection Gateway Proxy system, then create an identically-configured system and use a load-balancing proxy to distribute the load between these systems.

Before you begin

- ♦ Run the [Setup program](#) on each system. Use the **Features** tab to install the **Reflection Gateway Proxy** feature on each of these systems. Restart Windows on each system. This starts the services and creates initial default settings files.
- ♦ Log onto Gateway Administrator. Go to **System > File Servers** and confirm that **Transfer site file server** is set to use an added SFTP Server. Using the default Reflection Gateway Proxy is not supported for a high availability configuration because there is no replication of data between the Reflection Gateway Proxy systems.
- ♦ Select one of the Reflection Gateway Proxy systems for your initial configuration and testing. After you have this instance working, you will copy required files to duplicate the configuration on your other system.

Configure an initial Reflection Gateway Proxy system

- 1 Start the Reflection Secure Shell Proxy console on the server you are using for initial configuration.
- 2 On the **Reflection Gateway Users** pane, enable **Allow access to Reflection Gateway users**.
- 3 For **Gateway Administrator host**, enter the network name or IP address of the load-balancing proxy configured to connect to Reflection Gateway Administrator.
- 4 Click **Activate and verify**. Click **Yes** when prompted to restart the Reflection Transfer Server service.

This action configures the connection between components and saves an internal password that is used to connect to Gateway Administrator. (Each time you click **Activate and verify**, the internal password is changed.) Changes are saved to the following files: the Secure Shell Proxy's `trustedWebService.cer` and `RSITDatabase` files and the Transfer Server's `trustedWebService.cer` and `container.properties` files.

- 5 If your users will transfer files using the Transfer Client, you need to replace the default self-signed server certificate with a CA-signed certificate. See [“Replace the Default Server Certificate” on page 131](#). This certificate should be configured to authenticate the server name that will be used for connecting to your load-balancing proxy.
- 6 Test your configuration. Use Gateway Administrator to create Transfer Sites and confirm that you can transfer files using the Transfer Client or your alternate SFTP client.

Copy required configuration files to the duplicate Reflection Gateway Proxy system

You will need to copy configuration files for both the Reflection Secure Shell Proxy and the Reflection Transfer Server. These files are stored in different locations as described in the procedure.

- 1 On the destination server, stop the [Reflection Secure Shell Proxy \(page 141\)](#) and the [Reflection Transfer Server \(page 140\)](#) services.
- 2 Locate the Reflection Secure Shell Proxy configuration files. The default location is:

C:\ProgramData\Micro Focus\RSecureServer

3 Copy the following files to the duplicate system.

| File | Details |
|-----------------------|---|
| rssh_d_config.xml | The Reflection Secure Shell Proxy configuration file. The settings saved to this file include the values you have specified on the Reflection Gateway Users tab for connecting to the Gateway Administrator host name and port. |
| RSITDatabase | The Reflection Secure Shell Proxy's encrypted credential cache. |
| RSITDatabase.sec | This file contains the key required to decrypt the credential cache and is required to use the cache. |
| trustedWebService.cer | Contains the public key used to authenticate Reflection Gateway Administrator. This file is created when you click the Activate and Verify button on the Reflection Gateway Users pane. |
| hostkey | The private key of the public/private host key pair used to authenticate this server. |
| hostkey.pub | The public key of the public/private host key pair used to authenticate this server. |

4 Locate the Reflection Transfer Server configuration files. The default location is:

C:\Program Files\Micro Focus\ReflectionGateway\TransferServer

5 Copy the following files to the duplicate system.

| Files | Details |
|--|---|
| container.properties | In the <code>conf</code> subfolder. Includes settings and password for connecting to the Gateway Administrator. If configured, it includes settings for using a CA-signed certificate. |
| trustedWebService.cer | In the <code>etc</code> subfolder. Public key of Gateway Administrator. |
| servletcontainer.cer servletcontainer.bcfks | These files contain the certificate and private key used to authenticate the server when users make HTTPS connections to the Reflection Transfer Server. <ul style="list-style-type: none">◆ If you are using the default self-signed certificate, copy <code>servletcontainer.cer</code> and <code>servletcontainer.bcfks</code> located in the <code>etc</code> subfolder.◆ If you are using a CA-signed certificate, find the certificate package file in the location specified in the <code>container.properties</code> file. For example: <pre>servletengine.ssl.keystore=../etc/</pre>Copy this file to the same location on each of the other systems. |

6 Restart the Reflection Secure Shell Proxy and the Reflection Transfer Server on the duplicate system.

Related Topics

- ◆ [“Ensuring High Availability of Reflection Gateway Services” on page 143](#)

Sample HAProxy Configuration

The sample configuration files shown here provide examples of configuration for two [HAProxy](http://www.haproxy.org/) (<http://www.haproxy.org/>) load balancers. The proxy shown for use in the internal network supports both Jobs and Transfer sites. The proxy in the DMZ handles connections from Transfer Site users; it is not required for Jobs.

For a visual representation of proxy configuration, see the diagrams in “[Ensuring High Availability of Reflection Gateway Services](#)” on page 143.

Sample Proxy configuration in the internal network

This example shows settings to forward requests to two [identically configured Gateway Administrator servers](#) from browsers (port 9490), the Reflection Hub service (port 9186), and the Reflection Transfer Server service (port 9190).

```
global
    log 127.0.0.1    local0
    log 127.0.0.1    local1 notice
    maxconn 2384

frontend www-GA-https
    bind :9490
    mode tcp
    default_backend www-GA-backend

frontend www-HUB-to-GA-https
    bind :9186
    mode tcp
    default_backend www-HUB-to-GA-backend

frontend www-XFER-to-GA-https
    bind :9190
    mode tcp
    default_backend www-XFER-to-GA-backend

backend www-GA-backend
    mode tcp
    balance roundrobin
    stick-table type ip size 200k expire 30m
    stick on src
    default-server inter 1s
    server GA1-HTTPS 10.10.10.333:9490 check id 1
    server GA2-HTTPS 10.10.10.444:9490 check id 2

backend www-HUB-to-GA-backend
    mode tcp
    balance roundrobin
    default-server inter 1s
    server GA1-HUB 10.10.10.333:9186 check id 1
    server GA2-HUB 10.10.10.444:9186 check id 2

backend www-XFER-to-GA-backend
    mode tcp
    balance roundrobin
    default-server inter 1s
    server GA1-XFER 10.10.10.333:9190 check id 1
    server GA2-XFER 10.10.10.444:9190 check id 2
```

Sample Proxy configuration in the DMZ

This example shows sample settings to forward connections from Transfer Site users to two identically configured Reflection Gateway Proxy servers. Connections from the Reflection Transfer Client require forwarding of both HTTPS (port 9492) and SSH (port 22). Connections from alternate SFTP client requires forwarding of SSH only.

```
global
    log 127.0.0.1    local0
    log 127.0.0.1    local1 notice
    maxconn 2384

frontend www-Transfer-Client-https
    bind :9492
    mode tcp
    default_backend www-transfer-client-backend

frontend www-ssh-proxy
    bind :22
    mode tcp
    default_backend www-ssh-proxy-backend

backend www-transfer-client-backend
    mode tcp
    balance roundrobin
    stick-table type ip size 200k expire 30m
    stick on src
    default-server inter 1s
    server GP1-HTTPS 10.10.10.111:9492 check id 1
    server GP2-HTTPS 10.10.10.222:9492 check id 1

backend www-ssh-proxy-backend
    mode tcp
    balance roundrobin
    stick-table type ip size 200k expire 30m
    stick on src
    default-server inter 1s
    server GP1-SSH 10.10.10.111:22 check id 1
    server GP2-SSH 10.10.10.222:22 check id 1
```

Related Topics

- ◆ [“Ensuring High Availability of Reflection Gateway Services” on page 143](#)

Create an Audit Log of File Transfers

You can use audit logging to maintain a record of file transfer activity.

- ◆ To audit Transfer Site activity, set up audit logging on the Reflection Secure Shell Proxy.
- ◆ To audit Job actions that transfer files, you can use a Reflection for Secure IT Server as the SFTP server and set up audit logging on that server.

Both Reflection for Secure IT Server for Windows (one server is included with Reflection for Secure IT Gateway) and Reflection for Secure IT Server for UNIX (available separately) support audit logging. Use the procedure below to configure audit logging on a Reflection for Secure IT Server for Windows. On a Reflection for Secure IT Server for UNIX, use the AuditLog keyword to enable audit logging. See the [Reflection for Secure IT Server for UNIX User Guide \(http://support.attachmate.com/manuals/rsit_unix.html\)](http://support.attachmate.com/manuals/rsit_unix.html) for details.

NOTE: Auditing on these servers is not enabled by default.

The audit file is a comma-delimited text file with the following data for each transfer:

User ID
Client IP address
Action (upload or download)
Server filename
Start time
End time
Server file modification time
Server file size
Bytes transferred
Result (success or failure)
Reason
Server file hash (optional, the SHA-1 hash of the file contents)

To enable file transfer auditing

Use this procedure to enable audit logging on the Reflection Secure Shell Proxy or the Reflection for Secure IT Server for Windows.

- 1 Log in as an administrator to the Windows system on which you want to enable auditing. Use the Windows Start menu to launch the Reflection console:
 - ♦ To set up Transfer Site auditing, start the Reflection Secure Shell Proxy.
 - ♦ To set up auditing on a Reflection for Secure IT Server for Windows that is being used in Job actions, start the Reflection for Secure IT Server.
- 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, a new log is created each day in the specified **Audit log directory**. Audit logs use this name format: `RSSH-D-Audit-YYYYMMDD.log`, where `YYYYMMDD` indicates the date.

To view the audit log quickly from the console, use the audit log file toolbar button:



Change the JDK

The Reflection Transfer Server, Reflection Gateway Administrator, and Reflection Hub are Java applications. A correctly configured Java Development Kit (JDK) is installed and used by default. Use the procedures below to configure these services to use a different JDK.

NOTE: Each time you upgrade Reflection Gateway or apply a hotfix, you need to repeat the changes to the properties files.

Install a Java JDK from the Azul Zulu site

- 1 Go to the [Java SE Downloads page \(https://www.azul.com/downloads/\)](https://www.azul.com/downloads/).

2 Download and install the JDK.

- ◆ Download the latest Java 8 update.
- ◆ The Server JDK is recommended. This download does not include the browser plug-in. Because the browser plug-in is where most of the security vulnerabilities are found, using the server download helps reduce your security risk.

NOTE: Updates to Server JDKs you download this way are not automatic, and each update uses a new, version-specific folder (for example `C:\Program Files\Java\jdk1.8.0_nn\jre`).

Edit the properties files and restart the servers

1 Locate the configuration properties file (`container.conf`) for the service you are updating:

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

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

```
<install path>\Hub\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 JDK. For example:

```
wrapper.java.command=C:\Program Files\Java\jdk1.8.0_nn\bin\java
```

3 Restart the [Reflection Gateway Administrator \(page 140\)](#), [Reflection Transfer Server \(page 140\)](#), and [Reflection Hub \(page 141\)](#) services.

NOTE: You need to repeat this procedure each time you upgrade Reflection Gateway or apply a hotfix.

Glossary of Terms

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).

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.

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.

encryption. Encryption is the process of scrambling data by use of a secret code or cipher so that it is unreadable except by authorized users. Encrypted data is far more secure than unencrypted data.

Java keystore. A Java keystore is used for storage and transportation of certificates and associated private keys. Use the Java **keytool** utility to manage keystore files.

PKCS. PKCS (Public Key Cryptography Standards) is a set of standards devised and published by RSA laboratories that enable compatibility among public key cryptography implementations. Different PKCS standards identify specifications for particular cryptographic uses. Configuring certificates for Reflection Gateway you may work with the following PKCS file types.

PKCS#7 can be used to sign and/or encrypt messages. It can also be used to store certificates and to disseminate certificates (for instance as a response to a PKCS#10 message). Files in this format typically use a *.p7b extension.

PKCS#10 is used for certificate requests to a Certificate Authority (CA).

PKCS#12 is used for storage and transportation of certificates and associated private keys. Files in this format typically use a *.pfx or *.p12 extension.

X.509 certificate. See [“digital certificate” on page 153](#).

