MICRO FOCUS

Reflection for Secure IT Gateway

Evaluation Guide

version 1.1.2

Legal

Contents

Reflection for Secure IT Gateway

Reflection for Secure IT Gateway provides a secure, flexible way to manage files. Reflection for Secure IT 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.

General Features

- Web-based administration: The Gateway Administrator console is a web-based tool that enables administrators to modify Reflection Gateway system settings, provision users, and configure Jobs and Transfers.
- Delegated administration: The console supports delegation of management tasks. Administrators can assign roles to users or groups to allow limited access to the Gateway Administrator console features.
- Database options: Gateway Administrator installs with a default database, which stores Gateway data on the same system that runs the Gateway Administrator service. To support high availability in a production environment, you can configure Gateway Administrator to use a MySQL database running on a different system.
- End-to-end encryption: Reflection Gateway uses secure authentication and encryption throughout.
- File transfer auditing: The Reflection Gateway Proxy can be configured to maintain a complete record of all Transfer Site activity. Auditing of Job transfers can also be configured using a Reflection for Secure IT Server.
- Server options: You can configure Reflection Gateway to transfer files and/or execute commands on any SFTP-enabled SSH server. Authentication to your added SFTP servers can be configured using either password or public key authentication.

Jobs

Jobs are ideal for managing automated business-to-business processes. Use Jobs to monitor the content of a directory and initiate actions automatically when new files are added to the scanned directory, or existing files are updated. Because Job actions can trigger any command action supported on your servers, you can tie this feature to existing business practices and requirements. Jobs enable you to:

- Monitor directories on any added SFTP file server. You can specify which directory to scan and whether or not to include subdirectories.
- 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. Commands can be executed on the server where files first arrive, or on subsequent servers to which files are moved.

  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.

- 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.
- Manage access to servers using File Server Groups so that delegated Job administrators can configure Jobs on only those servers they have been granted access to.

Transfer Site Features

Reflection Gateway Transfer Sites are designed to support flexible, secure user-to-business file transfers. You can configure secure file exchange with business partners and/or employees working outside your corporate network. User authentication is required for all transfers and end-to-end encryption protects all transferred data. Features include:

- Choice of transfer client: Users can transfer files using the integrated web-based Transfer Client or any other SFTP-enabled SSH client available to them.
- Choice of authentication method: Configure user authentication using either password or X.509 certificate authentication.
- Customizable 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.
- LDAP integration: Windows Active Directory users can be added to Gateway Administrator. Authentication is managed by the LDAP server.
- 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.

Security Features

- Reflection for Secure IT Gateway uses the FIPS 140-2 “In Process” BCJFA 1.0.1 package from The Legion of the Bouncy Castle to establish secure sessions using the SSL/TLS protocol.
- The Reflection Secure Shell Proxy uses the OpenSSL FIPS Object Module v2.0.2 for FIPS 140-2 Level 1 validation (certificate #1747) and the OpenSSL Cryptography and SSL/TLS Toolkit version 1.0.2h.

1 A Sample Evaluation Scenario

Reflection Gateway is a flexible, secure way to manage file transfers. The evaluation scenario described in this guide touches on some of its key features. The procedures provided include step-by-step instructions for using each feature.

Meet Don

Don is in charge of evaluating Reflection Gateway for a growing financial services firm. Because secure encryption and authentication are built into every Reflection Gateway transfer, it is the ideal solution for ensuring the security of information exchanged with customers. The company requirements include the following:

- Don is looking for a secure method for analysts to use to distribute regular reports to customers.

  Reflection Gateway will be used to automate this process. Once the system is in place, all an analyst will need to do is drop a file into a specified folder on a server running in the internal network. Automated Reflection Gateway Jobs will handle the rest. Reflection Gateway's centralized management will make it easy for Don to add new employees to the system, and delegated administration will enable these employees to add new customers.
- Every document leaving the company network must first be scanned to ensure that outgoing content meets all security requirements of the company.

  The company has a working application that does this scanning, but the system is currently managed using scripts running on an increasing number of servers. Reflection Gateway will enable Don to set up centralized management of this process. This will simplify the process of updating scripts and adding new servers.
- To ensure the security of the company servers, analysts with access to the Reflection Gateway administrative tool should have limited rights.

  Reflection Gateway provides group configuration options to limit which administrative tasks users can perform and which servers they have access to.
- The company requires a complete audit log with of record of all transfer activity on the Transfer Site server.

Don's Evaluation Plan

Don plans on setting up the following test environment.

The players

- Don – The Principal system administrator for Gateway Administrator.
- Lee and Paul – Company employees with delegated file transfer management rights.
- Joe – A Customer

The systems

- Reflection Gateway server – For this evaluation all Reflection Gateway Services run on this single server.

- Report file server – Runs in the internal network. Reflection for Secure IT Server for Windows is installed on this server. Company employees will drop reports into a designated directory on this server.
- Transfer Site file server – Runs in the DMZ. Reflection for Secure IT Server for Windows is installed on this server. Files are exchanged from subdirectories of a designated base Transfer Site directory.

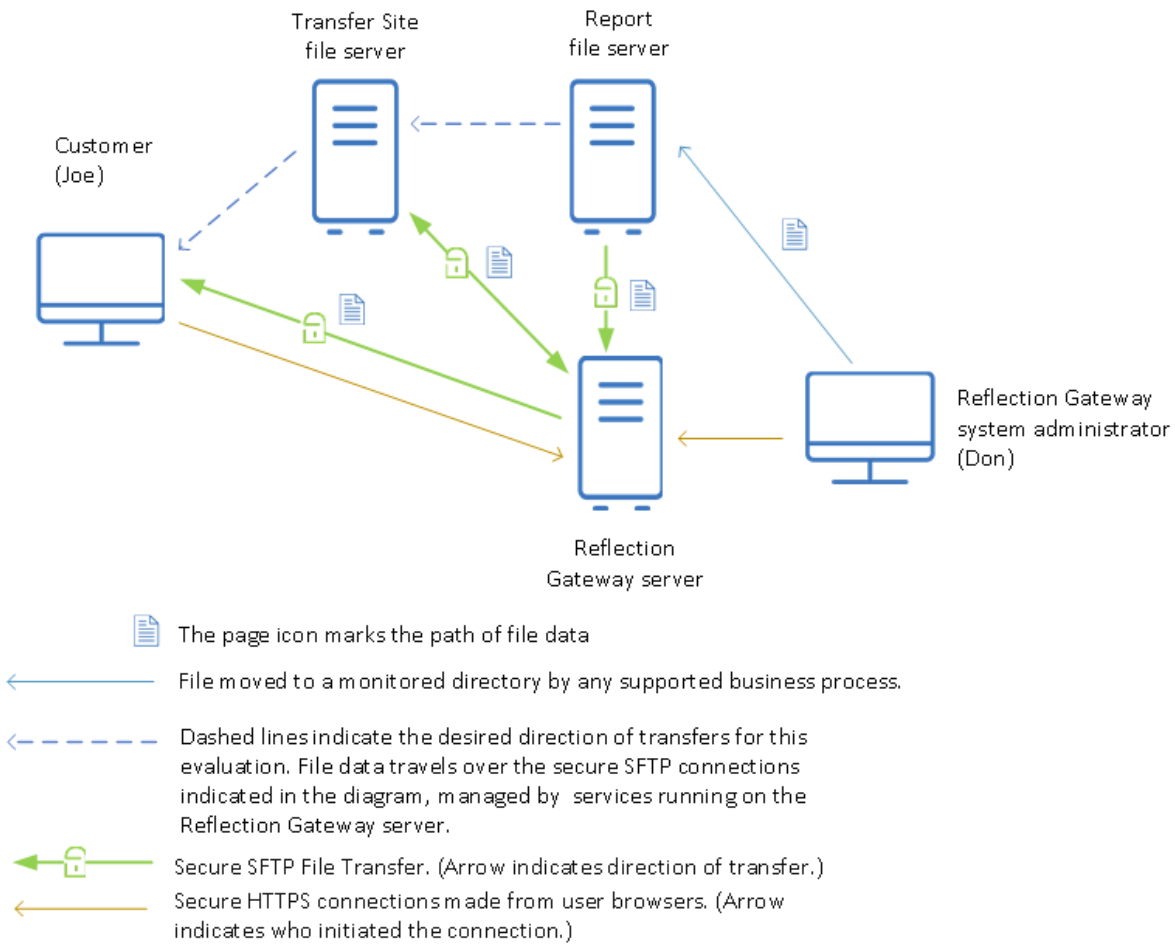
The test plan

Don will create a Reflection Gateway Job that monitors files on the Report file server, runs the company's security software on each file, and transfers files automatically to the Transfer Site file server only if they pass this security test.

Once the Job is tested and running, Don will configure a Transfer Site and add the customer (Joe) to the system so that he can access files from the Transfer Site file server. With these settings in place, he can drop a file in the designated folder on the Report file server. With no further action on his part, the file will be tested and moved to the Transfer site server.

The customer (Joe) will receive an email notification with a link that enables him to connect to the Reflection Transfer Client, which he can use to download the file.

After the test transfers are working as designed, Don will test features for delegating administrative tasks and limiting the access rights of delegated administrators. Finally, he will enable audit logging to provide a full record of all transfers.



The evaluation process

Don's evaluation will include the following procedures from this evaluation guide.

1. Install Reflection for Secure IT Gateway (page 11).

   The procedure provided in this guide uses a basic configuration, with all services Reflection Gateway Services on a single server (called the Reflection Gateway server in the diagram). Using this approach helps expedite preliminary testing. Multiple distributed configurations are also supported to meet the needs of your environment.

2. Configure the Report and Transfer Site file servers (page 12).

   This guide provides instructions for using the RSIT Server for Windows, which is included with the Reflection Gateway installer. Reflection Gateway also supports any SFTP-enabled SSH server. These can be UNIX as well as Windows servers.

3. Perform initial Reflection for Secure IT Gateway system setup (page 13).

4. Create a Job to run on the Report server (page 23).

   This job will monitor the analyst's drop-off directory for new or changed PDF files. It will run the security screening test on these files. After this test passes, the PDF files will be transferred to the Transfer Site server in the DMZ.

5. Create a Transfer Site and add the customer to this site (page 29).

   The file will be available to the customer from this site. An email notification will be sent to the customer with a link to use to download files using the Reflection Transfer Client. Don will receive an email notification when the customer downloads a new report.

6. Add delegated administrators and limit the rights of these users (page 33).

7. Configure file transfer audit logging on the Reports and Transfer Site servers (page 37).

2 Initial Setup

What You’ll Need for this Evaluation

- Reflection for Secure IT Gateway evaluation software. (See Install the Evaluation Software.)
- Three Windows servers that you can log into as an administrator. These can be virtual machines.
- Two different email addresses that you can access (one to receive administrative notifications and one to receive email messages aimed at the customer).

NOTE: For the easiest evaluation, have all servers behind your corporate firewall with no firewall restrictions between them.

To see what ports would need to be open in a distributed production environment, see Ports and Firewall Configuration (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/fxg_ports.htm) in the Administrator’s Guide.

Install the Evaluation Software

For this evaluation, you'll install all Reflection Gateway services on a single system.

Install an evaluation copy of Reflection for Secure IT Gateway

1. Log in as an administrator on the Windows system that will serve as your Reflection Gateway server for this evaluation.
2. Go to the evaluation download page (https://www.attachmate.com/products/reflection/reflection-for-secure-it-gateway-eval-form.html). Enter the requested information, and click **Submit**. You will receive an email message with download instructions.
3. Download and launch the package. Select a location for the installer files. (For this evaluation, you might want to select a shared network location to be able to access the Setup program again when you install the Reflection for Secure IT Server.) Click **OK**. The files are extracted to the specified location, and the Setup program starts.
4. 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 installation continues after this prerequisite is installed.
5. Install using defaults. This installs all four services.
6. Select the option "Restart my computer for me."

A Windows restart is required to complete the installation. It also starts the Reflection for Secure IT Gateway services.

7 To confirm that the services are installed and running, you can use the Windows Services console. The following four services should be present and running: Micro Focus Reflection Gateway Administrator, Micro Focus Reflection Hub, Micro Focus Reflection Secure Shell Proxy, and Micro Focus Reflection Transfer Server.

Do more...

This evaluation uses a single server running all the services. To learn about setting up a distributed configuration, see these topics in the Administrator's Guide:

- Reflection for Secure IT Gateway Components (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/gateway-components.htm)
- Changing the Gateway Administrator Database (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/change-ga-database.htm)
- Ensuring High Availability of Reflection Gateway Services (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/fxg_clusters.htm)

Set Up SFTP File Servers

This evaluation uses two SFTP file servers, the Reports server and the Transfer Site file server. The instructions given here use the Reflection for Secure IT Server for Windows.

NOTE

- A single license to run Reflection for Secure IT Server for Windows is included with Reflection for Secure IT Gateway. This server is included in the Reflection for Secure IT Gateway installer. For the exercises in this guide, you will install this evaluation software on two servers.
- Using a Reflection for Secure IT Gateway server is not a requirement of; you can configure Reflection Gateway to work with any SFPT-enabled SSH server.

Set up the Reports Server

The Reports server for this evaluation represents the server in the internal network where analysts will first place their reports. For this evaluation, this server needs an accessible reports directory.

Install Reflection for Secure IT Server for Windows on the server

1 Log into the Windows system using administrator credentials. Make a note of these credentials. You will use them later to configure access to this system from the Gateway Administrator console.

2 Run the evaluation Setup program from the location where you expanded the download package.

3 Install the Reflection for Secure IT Server for Windows.

To install just this feature, click the **Feature Selection** tab. Deselect each of the default services (click the icon next to the feature name and select **Feature will be unavailable**) and select **Reflection for Secure IT Server** (click the icon and select **Feature will be installed on local hard drive**.)

4 Restart Windows to complete the installation and start the Reflection for Secure IT Server service.

Create an accessible reports directory

1 Create a folder called `reports` in the root of this server's file system (`c:\reports`).
2 Start **Reflection for Secure IT Server** from the Windows start menu,
3 From the **Configuration** tab, select **SFTP Directories** and click **Add**.
4 For **Virtual directory** enter `reports`.
5 For **Local or UNC directory** enter `c:\reports`.
6 Click **OK**.
7 Save your settings (**File** > **Save Settings**).

Set up the Transfer Site File Server

You will configure a Job to move files automatically from the Reports server to the Transfer Site file server. For this evaluation, Transfer Site files will be stored in a folder called `c:\gateway`.

Install Reflection for Secure IT Server for Windows on the server

1 Install an evaluation copy of Reflection for Secure IT Server for Windows on this server as you did on the Reports server. Make a note of the credentials required to log onto this Windows system.
2 Restart Windows.

Create an accessible gateway directory

1 Create a folder called `gateway` in the root of this server's file system (`c:\gateway`).
2 Start **Reflection for Secure IT Server**, from the Windows start menu,
3 From the **Configuration** tab, select **SFTP Directories** and click **Add**.
4 For **Virtual directory** enter `gateway`.
5 For **Local or UNC directory** enter `c:\gateway`.
6 Click **OK**.
7 Save your settings (**File** > **Save Settings**).

Gateway Administrator System Setup

The initial setup procedures introduce you to Gateway Administrator, a web-based tool for provisioning users and configuring Jobs and Transfer Sites.

- "Log on to Gateway Administrator" on page 14
- "Add File Servers" on page 14
- "Add a Hub" on page 17

- “Set Up Email” on page 17
- “Add Users” on page 19

Log on to Gateway Administrator

You’ll do the initial configuration by logging in with the default *admin* account.

To connect to the Gateway Administrator and log on

1 Start Gateway Administrator. For your initial tests, you can start it from Windows Start menu on the server running the Reflection Gateway services (**Micro Focus > Reflection for Secure IT Gateway > Reflection > Gateway Administrator**).

You can also connect directly to Gateway Administrator from a browser on any system with access to your server by pointing to the server address at port 9490, as shown here:

```
https://GatewayServer: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 detailed information about installing a certificate from a trusted Certification Authority, see Server Certificate Management (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/fxg_certificates_ch.htm) in the Administrators Guide.

---

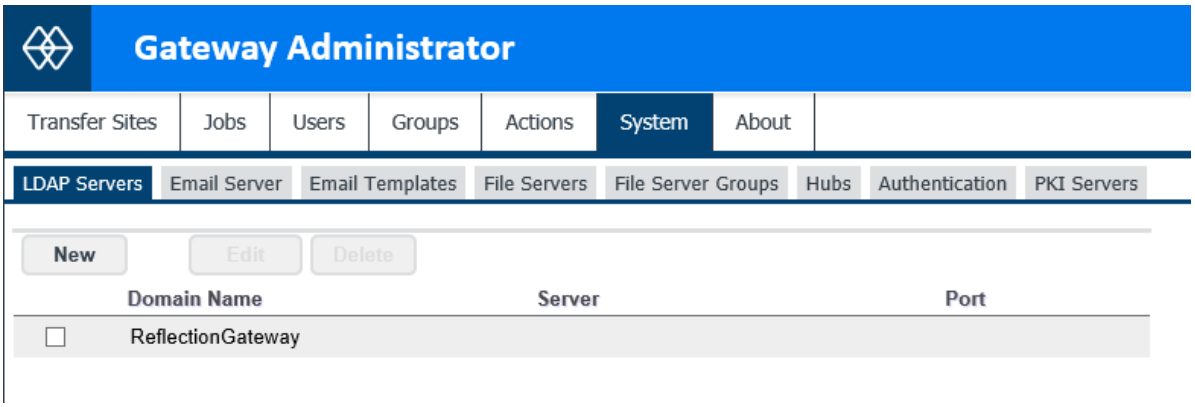
2 For your initial logon, enter the following credentials:

Username: `admin`

Password: `secret`

3 Immediately after your first logon, you will be prompted to change the password for the admin account. This account has access to all Gateway Administrator features.

4 Click the **System** tab to view the system configuration features:



Add File Servers

These procedures enable Gateway Administrator to connect to your SFTP file servers.

Add the Reports File Server

1 If you are not still logged in, log on to Gateway Administrator using the default *admin* account.

2 From the **System** tab, click **File Servers**, then click **New**.

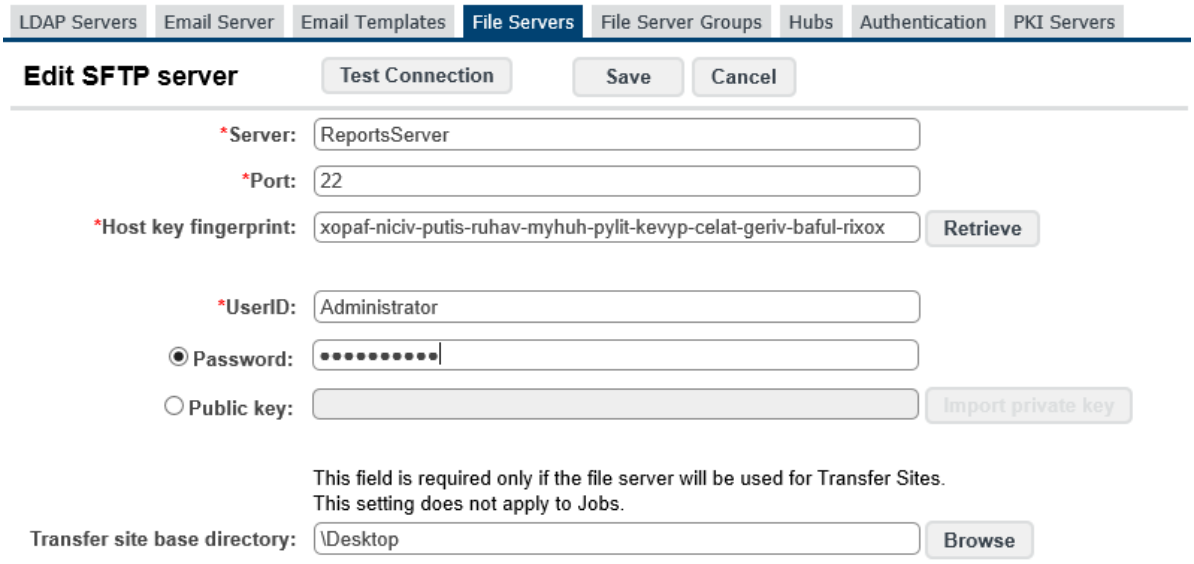
3 Enter the server name (or IP address) of your Reports server.

4 Click **Retrieve** to retrieve the host key.

5 For **UserID** and **Password** enter the Windows user credentials for this server.

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

7 Click **Save**.

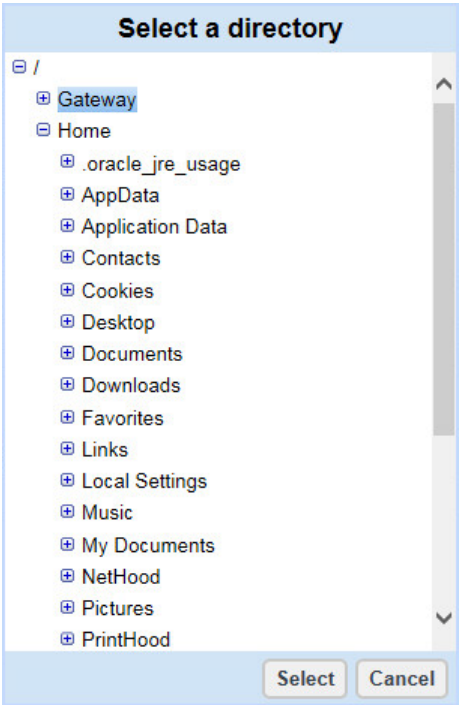


Add the Transfer Site File Server

1 From the **File Servers** tab, click **New**.

2 Enter the server name or IP address of your Transfer Site server, retrieve the host key, enter user credentials for this server, and test the connection.

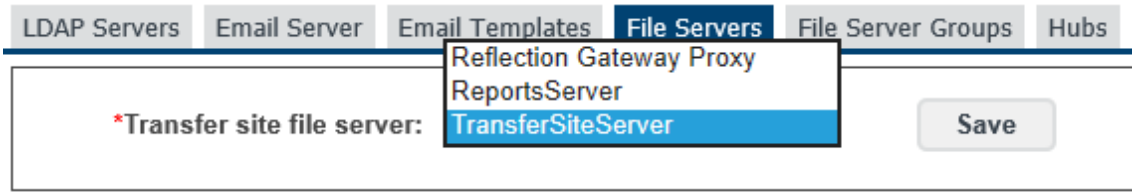
3 Next to **Transfer site base directory**, click **Browse**. Select the `Gateway` directory that you made accessible on this server, and click **Select**.



This sets the **Transfer Site base directory** for this server. By default, Gateway Administrator uses a Reflection subdirectory in the selected directory:

4 Click **Save**. This returns you to the **File Servers** tab.

5 Use the **Transfer site file server** drop-down list to select the server you just added and click **Save**.



Do more...

- For this evaluation we are using passwords to authenticate to the added SFTP servers. Reflection Gateway also supports public key authentication. See Add File Servers to Gateway Administrator (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/sftp-server-setup-pr.htm) in the Administrator's Guide.

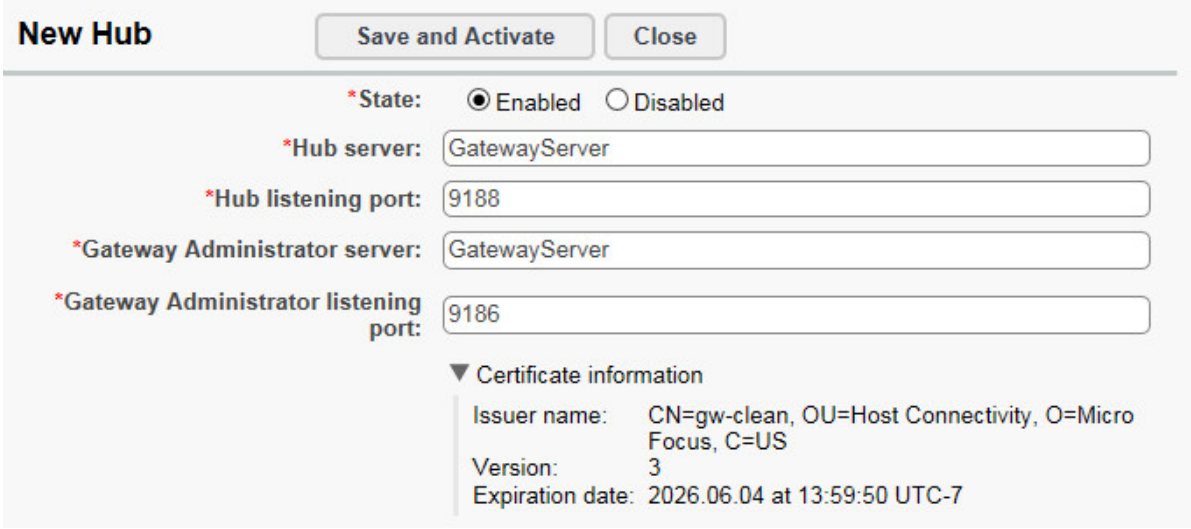
Add a Hub

The Reflection Hub service manages Jobs. You can install this service on one or more systems. For this evaluation a single Hub service is running on the same system as Reflection Gateway.

To add a Hub

1. Log onto Gateway Administrator using the default *admin* account.
2. Go to **System** > **Hubs** and click **New**.
3. For **Reflection Hub server**, enter the name or IP address of the system on which you installed the Reflection Gateway services. The correct default listening port is entered automatically.

   The correct name and port for the Reflection Gateway Administrator service are entered automatically.
4. Click **Save and Activate**. This step sets up a trust relationship between the Hub and Reflection Gateway Administrator servers using digital certificates.

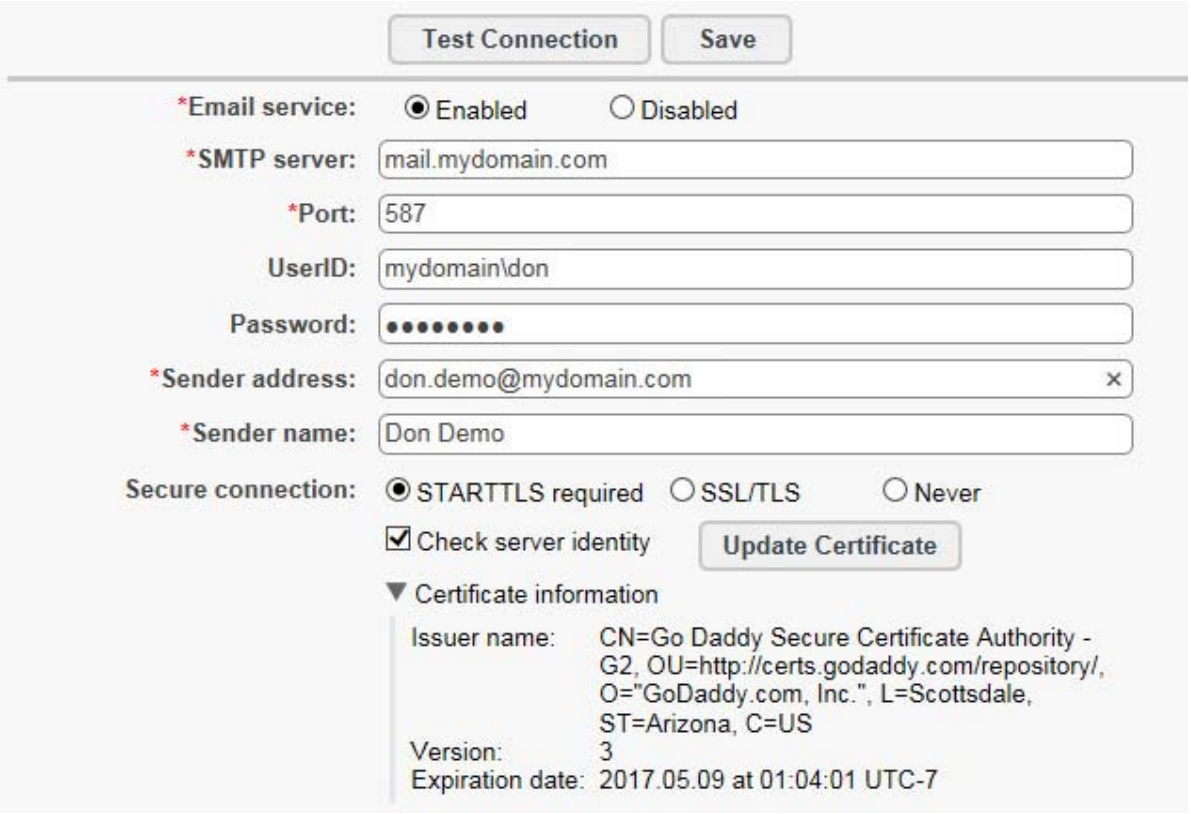


Set Up Email

Reflection Gateway supports a number of optional email notification services. The procedures in this guide demonstrate how to configure a number of email notifications. To support these services, you need to configure access to an email server and also configure the server address that will be used in URL links included in email messages.

Configure the email server connection

1. Log onto Gateway Administrator using the default *admin* account.
2. Go to **System** > **Email Server**, click **Enabled**, then enter values for connecting to your email server.
3. Click **Retrieve Certificate**.
4. Click **Test Connection**. (This tests the current on-screen settings. These settings are not saved until you click **Save**.)
5. 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.

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.

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. In this evaluation, you will create Transfer Sites that use these emails. To support this feature from any workstation, you need edit to replace localhost a server name or IP address.

Configure the base server URL used in Transfer Site email message links

For this procedure you will edit a text settings file, then restart the Gateway Administrator service.

1. Log out of Gateway Administrator .
2. 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
   ```

3. Locate the following lines:

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

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

```
transfer.server.url=https://gatewayserver.mydomain.com:9492
```

5 Save the edited properties file.

6 Open the Windows Services console and restart the Gateway Administrator service. A restart is required after any changes to the properties file.

NOTE: It make take up to several minutes after the restart before you can log in again to the Gateway Administrator. .

Add Users

For the initial setup, we'll add two users:

- Don - Our evaluating system administrator will have full access to all Gateway Administrator features.
- Joe - Our sample customer will have access to the Transfer Client, but not Gateway Administrator.

NOTE: Each email address in the ReflectionGateway user list must be unique. To see emails for each sample user, use two different email addresses that you can access.

To add Don as a full administrator

1 Log into Gateway Administrator using the default *admin* account.

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

3 For **UserID** enter *Don*.

4 For **Email address** enter an email address that you can access.

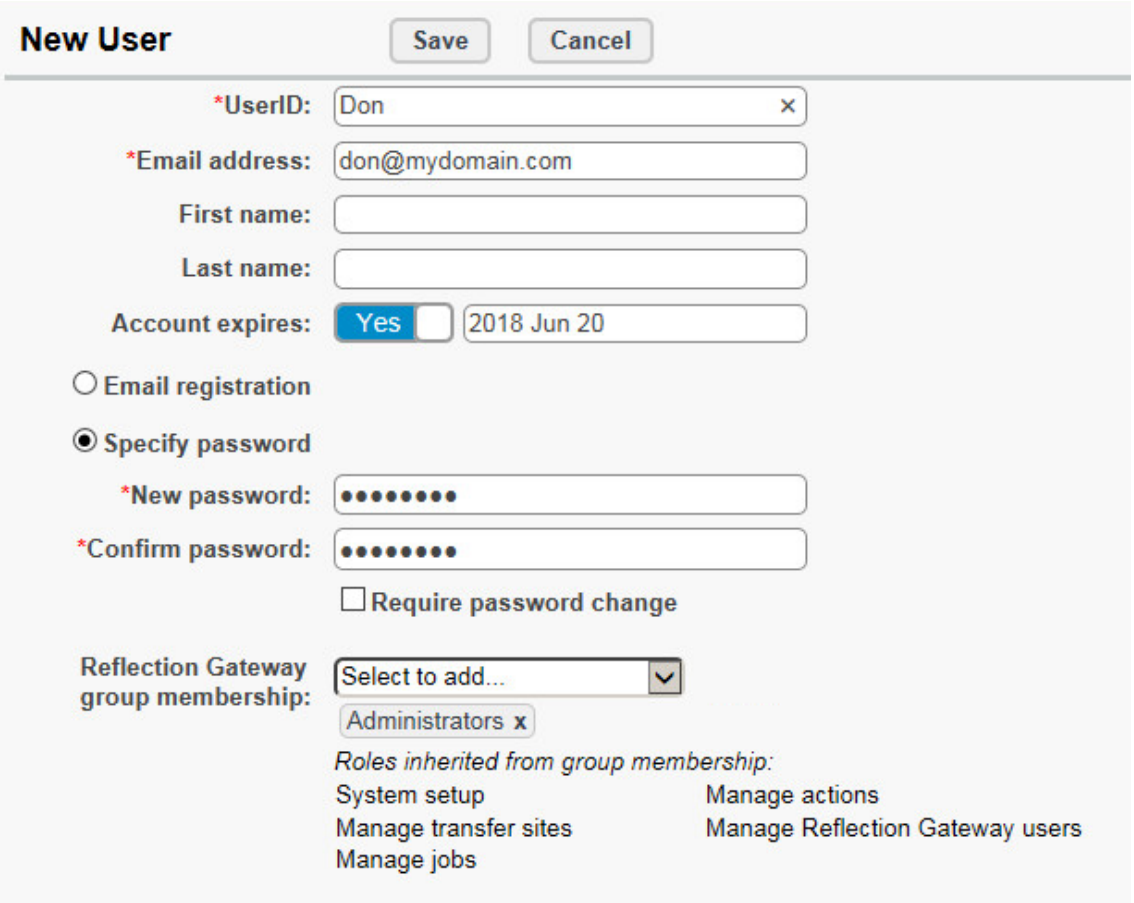
5 Click **Specify password**, then enter and confirm a password (it must be at least 8 characters long).

NOTE: Email registration is not available for users who will have access to the Gateway Administrator console.

---

6 From the **Reflection Gateway group membership** list, select **Administrators**.

This group provides access to all available roles, and these are listed beneath the group name.



7 Click **Save**.

To add Joe

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

2 For **UserID** enter *Joe*.

3 For **Email address** enter a second email address that you can access.

4 Click **Specify password**, then enter and confirm a password (it must be at least 8 characters long).

5 Click **Save**.

6 Click the **Logout** button in the upper right to log out of the default admin account.

7 Try logging into Gateway Administrator as *Joe*. Note that this user who has no Gateway Administrator roles assigned cannot log in.

Do more...

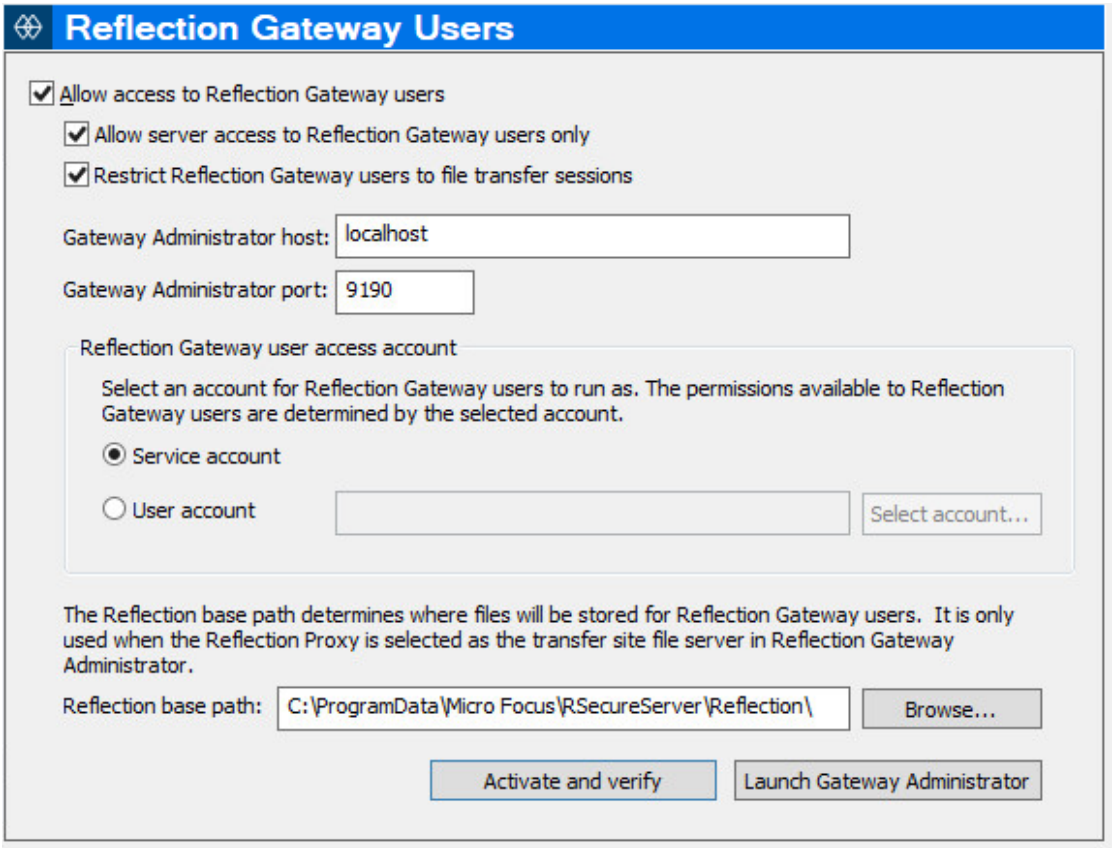
- You can use Reflection Gateway's LDAP integration to provision users who have accounts in Windows Active Directory. See Provision Users from an Added LDAP Server (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/fxg_add_ldap_users.htm) in the Administrator's Guide.
- By default, users log on to the Transfer Client with a user name and password. You can also configure authentication using X.509 certificates, which may be on a Smart Card or configured on user systems. See *Configure Certificate User Authentication* (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/fxg_configure_cert_authentication.htm) in the Administrator's Guide.

Reflection Secure Shell Proxy Setup

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

To set up the Reflection Secure Shell Proxy to support Transfer Sites

1. Use the Windows Start menu to launch the Reflection Secure Shell Proxy console (**Reflection for Secure IT Gateway** > **Reflection Secure Shell Proxy**).
2. On the **Reflection Gateway Users** pane, enable **Allow access to Reflection Gateway users**.
3. For **Gateway Administrator host**, you can leave the default (localhost) for this evaluation. In a distributed environment, you would enter the name or IP address of the computer running the Reflection Gateway Administrator. Leave the default port value (9190). Reflection Gateway Administrator is configured to listen on this port by default.
4. Click **Activate and verify**. This saves your settings and triggers actions that ensure that the 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.


Reflection Gateway Users
Allow access to Reflection Gateway users
Allow server access to Reflection Gateway users only
Restrict Reflection Gateway users to file transfer sessions
Gateway Administrator host:
localhost
Gateway Administrator port:
9190
Reflection Gateway user access account
Select an account for Reflection Gateway users to run as. The permissions available to Reflection Gateway users are determined by the selected account.
Service account
User account
Select account...
The Reflection base path determines where files will be stored for Reflection Gateway users. It is only used when the Reflection Proxy is selected as the transfer site file server in Reflection Gateway Administrator.
Reflection base path:
C:\ProgramData\Micro Focus\RSecureServer\Reflection\
Browse...
Activate and verify
Launch Gateway Administrator

3 Set Up Automated Job Actions

In this part of your evaluation, you will create a Reflection Gateway Job that monitors files on the Report file server and runs a test command on each file. Once you have this working, you'll add a second job action that transfers files automatically to the Transfer Site file.

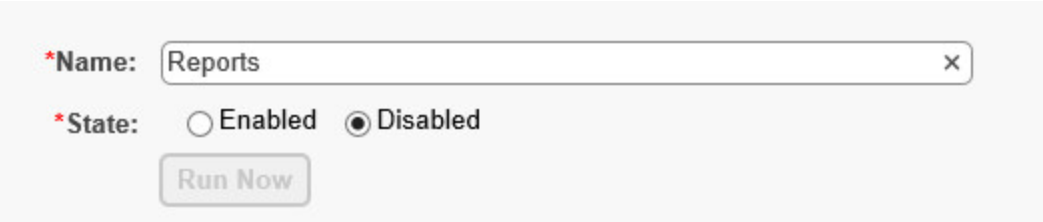
Be sure you've completed all initial setup steps before you begin.

Create a Job Action that Executes a Command

For this demonstration we'll use a system command as a stand-in for the security software required by Don's company. The command will save the filename and time to a text file. If this succeeds, we'll consider the file "safe." In the real world, this command could be replaced by any security software your company needs to run.

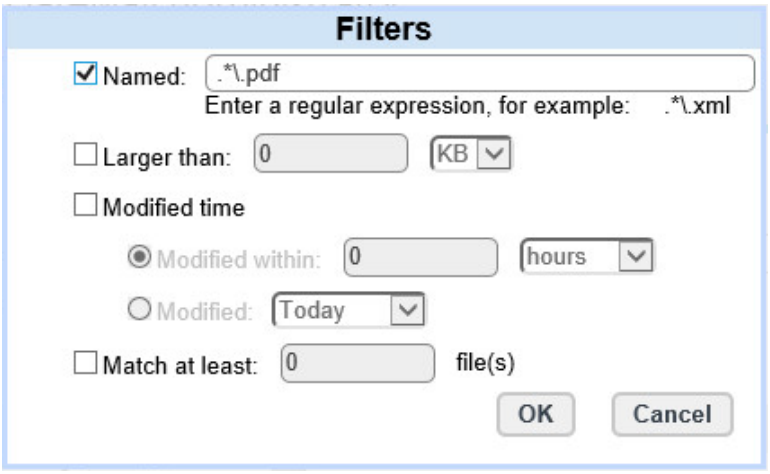
Create a Job to screen outgoing reports

1. Log into Gateway Administrator as *Don* using the password you specified when you created this account.
2. Go to **Jobs** > **New**.
3. For **Name** enter *Reports*.
4. For **State**, 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, you can select **Enabled** to run the Job at the specified scan interval.



5. Under **Source Files**, select the SFTP server on which you created the accessible `c:\reports` directory. Click Browse and select the `reports` directory. This sets up the directory to be scanned. Any new or updated files in this directory will trigger the Job actions you configure.

6 For this test, we want to scan and move only PDF documents. To do this, next to **Filters**, click **Change...**. Select **Named** and enter `.*\.pdf` in the text box. This regular expression filters for all files with a pdf file extension. Check to be sure you've entered it correctly, including both periods.



Click **OK** to return to the **New Job** page.

7 Under **Actions**, from the **Add action...** drop-down list, select **Execute command**. In the Execute Command dialog box, for Server, select your Reports Server. For Command, enter the following:

```
cmd /c echo $FILENAME$ $DATE$ $TIME$ >> c:\reports\safefiles.txt
```

This command will be our stand-in for a security test. For the purposes of this demo, if files can be successfully written to `safefiles.txt`, the test passes.

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

Click **OK** to return to the **New Job** page.

8 Under **Success**, click **Change** to configure email notifications. In the Success Action dialog box, click **Enabled** and enter the email address you used for Don's account. Use the **Tokens** button to add the JOB_NAME token. It will be replaced with the Job name in the email message:

Click **OK** to return to the **New Job** page.

9 Create a **Failure Action** in the same way.

10 Click **Save**.

Test your Job

1 On the Reports server, copy one or more `*.pdf` files to `c:\reports`.

2 In Gateway Administrator, go to the **Jobs** page, select the *Reports* Job and click **Edit**.

3 Click **Run Now** to test the action. You'll see a Running Job message. This tells you the Job has been initiated. You can close this message at any time; it has no effect on execution of Job actions.

If the Job works, you should see a new file called `safefiles.txt` in the `reports` folder on your Reports server and you should receive a success notification in the email you specified.

If your Job did not work as expected, review these instructions, or refer to the testing notes (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/job-action-testing.htm) and troubleshooting (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/job-troubleshooting.htm) help in the Administrator's Guide.

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

Make a copy of the working Job

After you get your Job working, you can make a copy of it and use the copy to experiment. When you're ready to continue with the procedures in this guide, you can return to the original Job.

1. In Gateway Administrator, go to the **Jobs** page, select the *Reports* Job and click **Copy**.
2. Confirm that you want to make the copy. This creates a new Job called *Reports_copy1*.

Add an Action that Transfers Files

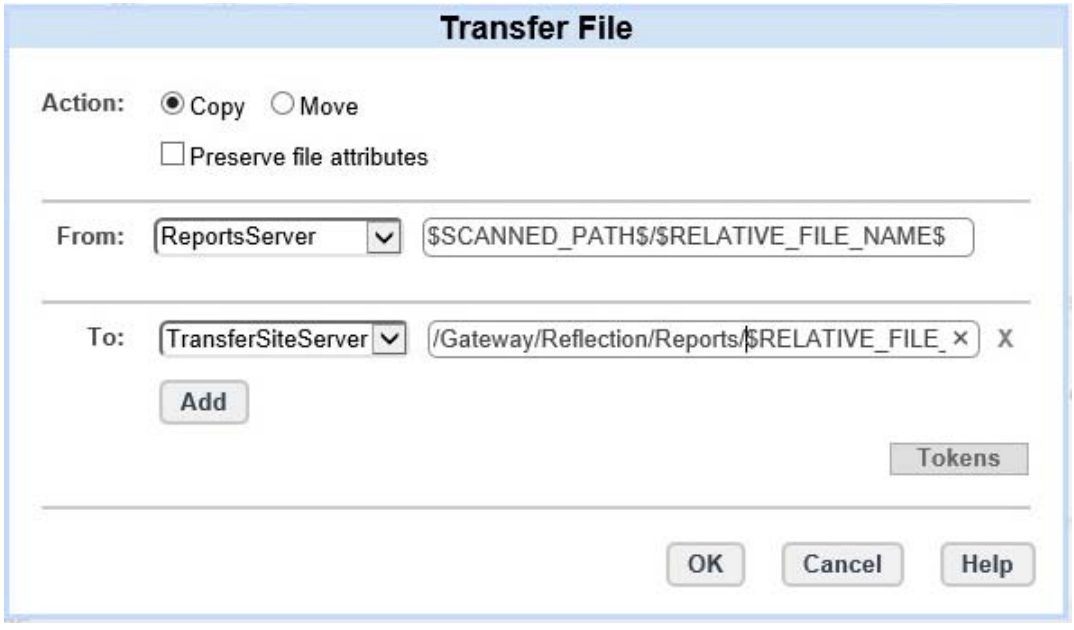
After you have the stand-in security test working, you're ready to create a second Job action that moves the files to your Transfer Site server.

To add a Job action that Transfers Files

1. If you are not still logged in, log into Gateway Administrator as *Don*.
2. From the **Jobs** page, select the *Reports* Job and click **Edit**.
3. Under **Actions**, from the **Add action...** list, select **Transfer file**.
4. For **From**, leave the default values.
5. For To, select the name of your Transfer Site file server and enter the following path:

   `/Gateway/Reflection/Reports/$RELATIVE_FILE_NAME$`

   The first part of the path (`/Gateway/Reflection`) identifies the Transfer Site base directory you specified for this server. Putting files in a subdirectory of this directory will enable you to create a Transfer Site later for exchanging these files.



Click **OK** to return to the **New Job** page.

Test your modified Job

1. On the Reports server, copy one or more `*.pdf` files to `c:\reports` or update the existing files.

   NOTE: To facilitate testing, you can quickly update your files from a Command Window using the `copy` command with the syntax shown here:

   ```
   C:\reports> copy /b *.pdf +,,
   test.pdf
   test2.pdf
           2 file(s) copied.
   ```

2. In Gateway Administrator, go to the **Jobs** page, select the Report Job and click **Edit**.
3. Click **Run Now** to test the action. You'll see a Running Job message. You can close this message at any time; it has no effect on execution of Job actions.

If the Job works, you should receive a success notification in the email you specified. Go to your Transfer Site server and confirm that your PDF files have been transferred to `C:\Gateway\Reflection\Reports`. Note that `safefiles.txt` was not included in the transfer because it does not meet the filter requirements.

Ensure that the Job Stops if the Security Test Fails

For this Evaluation, Don wants to be sure that files that do not pass the company's security test are not moved to the Transfer Site server in the DMZ. To mimic this circumstance in our evaluation setup, we'll make the `safefiles.txt` file read-only. When the Job command action tries to write to this file, the action will fail. Because the first Job action fails, no subsequent actions will run and you should get a failure email notification.

Test the Job with a command failure

1. On the Reports file server, locate `safefiles.txt`, which was created by earlier tests in this location:

   `c:\Reports\safefiles.txt`
2. Make this file read-only (right-click > **Properties** > **Read-only**).
3. Copy one or more new `*.pdf` files to `c:\Reports` or update the existing files.
4. Return to Gateway Administrator. If you are not still viewing the *Reports* Job, select it from the **Jobs** page and click **Edit**
5. Click **Run Now**.

   This time you should receive a failure email notification.

   On the Transfer Site server, confirm that no new files were transferred to the Transfer Site directory (`C:\Gateway\Reflection\Reports`).
6. After you've confirmed the failure case, return to the Reports file server and delete the read-only copy of `safefiles.txt` (or make it writable) so subsequent Jobs will succeed.

Test the Job again to be sure it is running successfully before you continue with the evaluation.

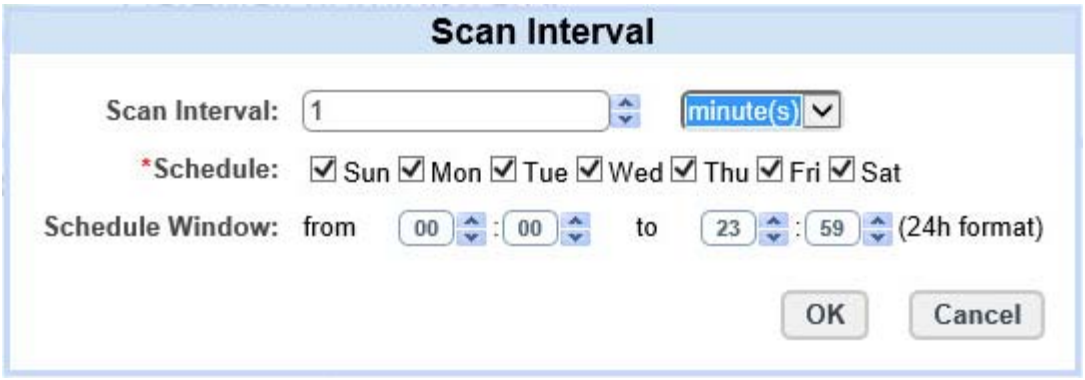
Start Automatic Scanning

After you confirm that a Job is working using the **Run Now** button, you can set it up to scan the directory on a regular interval and trigger Job actions automatically when files that meet your filter conditions are added or updated.

Set a scan interval and enable the Job

1. If you are not still viewing the *Reports* Job, select it from the Gateway Administrator **Jobs** page and click **Edit**.
2. Set **State** to **Enabled**.
3. Next to **Scan Interval**, click **Change**.

   For this test the **Scan Interval** to 1 minute. Then click **OK** to return to the **Edit Job** page.



4. Click **Save & Close**.
5. Go to your Reports server and copy one or more new `*.pdf` files to `c:\Reports` or update the existing files.

After a wait of a bit more than a minute, you should receive a success email. Confirm that the file name(s) are added to `successfiles.txt` on Reports server and the files have been transferred to the Transfer Site server.

4 Set Up a Transfer Site

In this part of the evaluation you will create a Transfer Site and a new user in Gateway Administrator –the customer named Joe. After you've set this up, you will be able to launch the Transfer Client in a web browser and use it to download the PDF files that were put there by your automated Job actions.

Before you begin

- Confirm that the user called Joe has been added and configured to use an email address you have access to.

NOTE: The Reflection Transfer Client is used here to access Transfer Sites, but this is not a requirement. You can also use the Reflection for Secure IT Client for Windows, the Reflection FTP Client configured for SFTP transfer, or any other SFTP-enabled SSH client.

- "Create a Transfer Site" on page 29
- "Connect to the Transfer Client" on page 30
- "Test the Complete File Transfer Pathway" on page 32

Create a Transfer Site

In this procedure you will create a Transfer Site called *Reports*. This site will initially have two members. The system administrator, Don, who creates the site will have management rights and full access to upload and download files. The customer, Joe, will receive email notification when he is first given access to the site and will have rights to download files only.

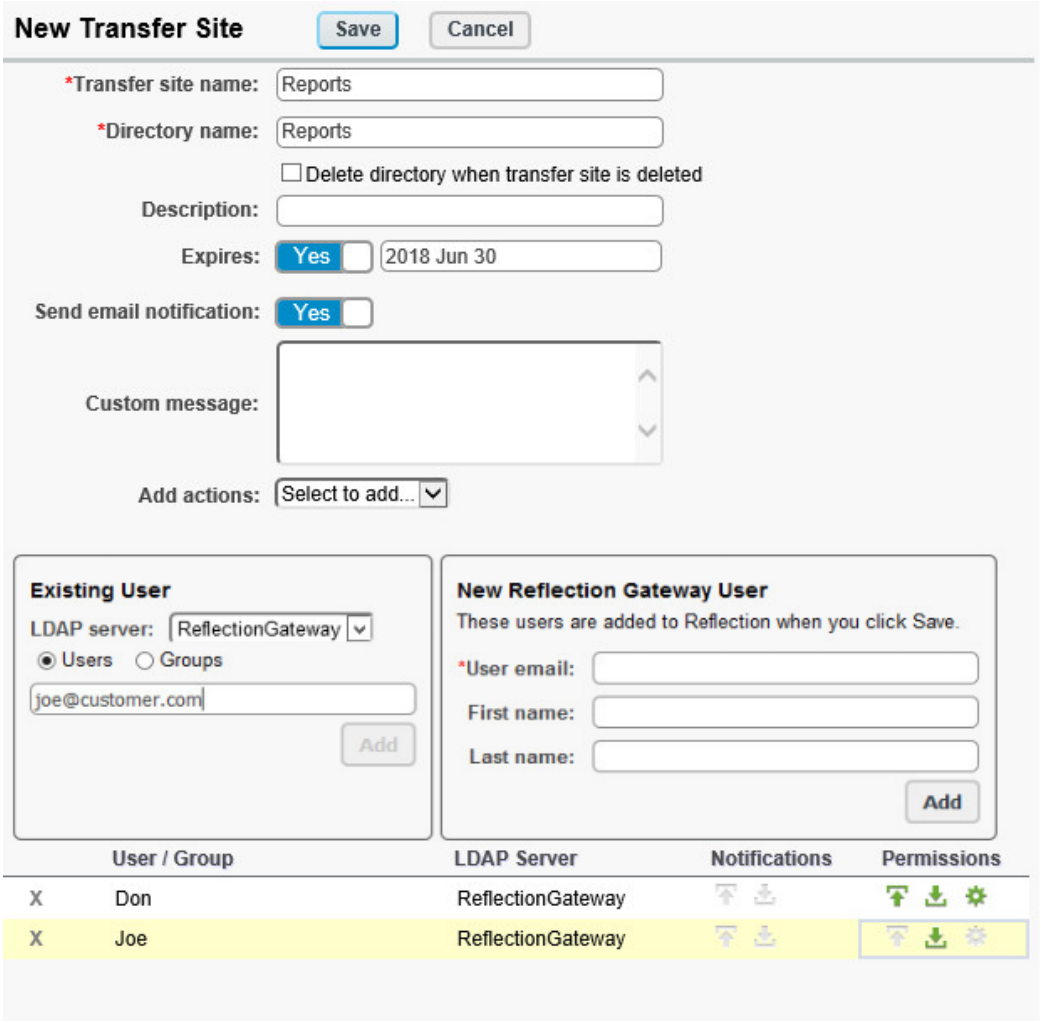
Add a new Transfer Site

1. Log into Gateway Administrator as *Don*.
2. From the **Transfer Sites** page click **Add.** This opens the **New Transfer Site** page.
3. For **Transfer site name**, enter *Reports*

   Click in **Directory name** to enter this same name automatically.

   The Job you have already configured and tested uploads files to `c:\Gateway\Reflection\Reports`. Because the Transfer Site base directory is `c:\Gateway\Reflection`, specifying `Reports` for the directory here will give Transfer Site users access to the files uploaded to that location by your Job.
4. Under **Existing User**, type *Joe* in the search box. When you see the email address you provided for this user, select it and click **Add**. (Email addresses are shown because these are always unique for each user.)

   This adds Joe to the list of users for this Transfer Site.
5. For *Joe*, under **Permissions**, click the upload icon to change it from green (enabled) to gray (disabled). This change disables his ability to upload files.



6 Click **Save**.

You'll see a message telling you that the specified directory already exists on your server. This directory was created by the automated Job you've already tested. Click **OK**. For this test, this message confirms that the configuration is what we want.

Connect to the Transfer Client

The Reflection Transfer Client is a Java applet that runs in a web browser. Before you do the next procedure, confirm that Java is installed and enabled on the system you are using for testing. For this test you want Java running on default browser running on the system where you will receive Joe's email.

To verify that Java is installed

NOTE: Java is not supported on current releases of Chrome.

---

1 Go to the Oracle Java website (http://www.java.com).

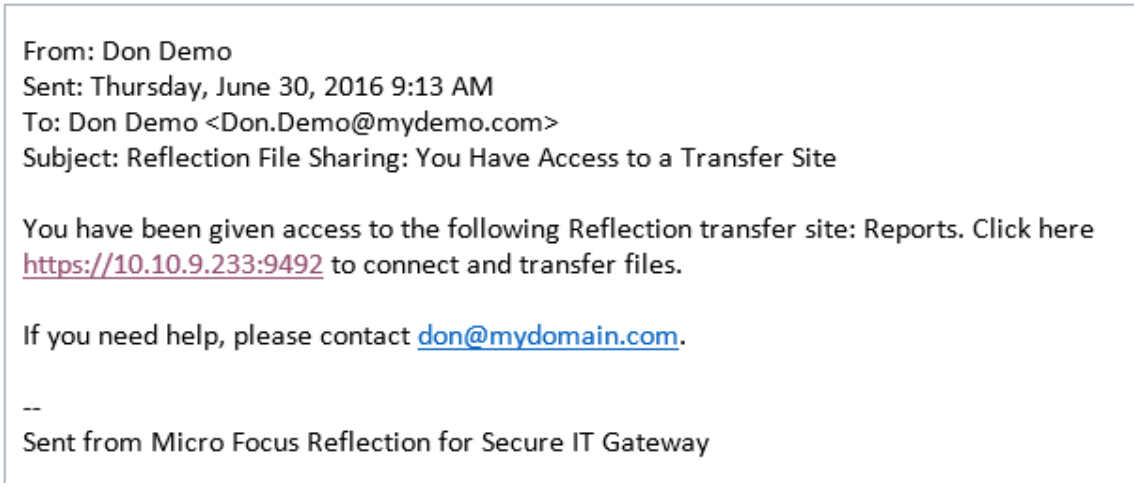
2 Click **Do I have Java?** then **Verify Java version** to verify that Java is installed and activated.

3 If you are not running Java, use the **Free Java Download** to download and install it.

If you prefer to test with a different client, see the alternate instructions provided in the Administrator's Guide (https://www.attachmate.com/documentation/gateway-1-1/gateway-admin-guide/data/alt-transfer-client.htm).

Connect to the Transfer Client using the customer account

1 Open the email account you used for Joe. You should see an email like the following with the subject heading, "Reflection File Sharing: You Have Access to a Transfer Site."



From: Don Demo
Sent: Thursday, June 30, 2016 9:13 AM
To: Don Demo <Don.Demo@mydemo.com>
Subject: Reflection File Sharing: You Have Access to a Transfer Site

You have been given access to the following Reflection transfer site: Reports. Click here https://10.10.9.233:9492 to connect and transfer files.

If you need help, please contact don@mydomain.com.

--
Sent from Micro Focus Reflection for Secure IT Gateway

2 Click the link in the email to launch the browser.

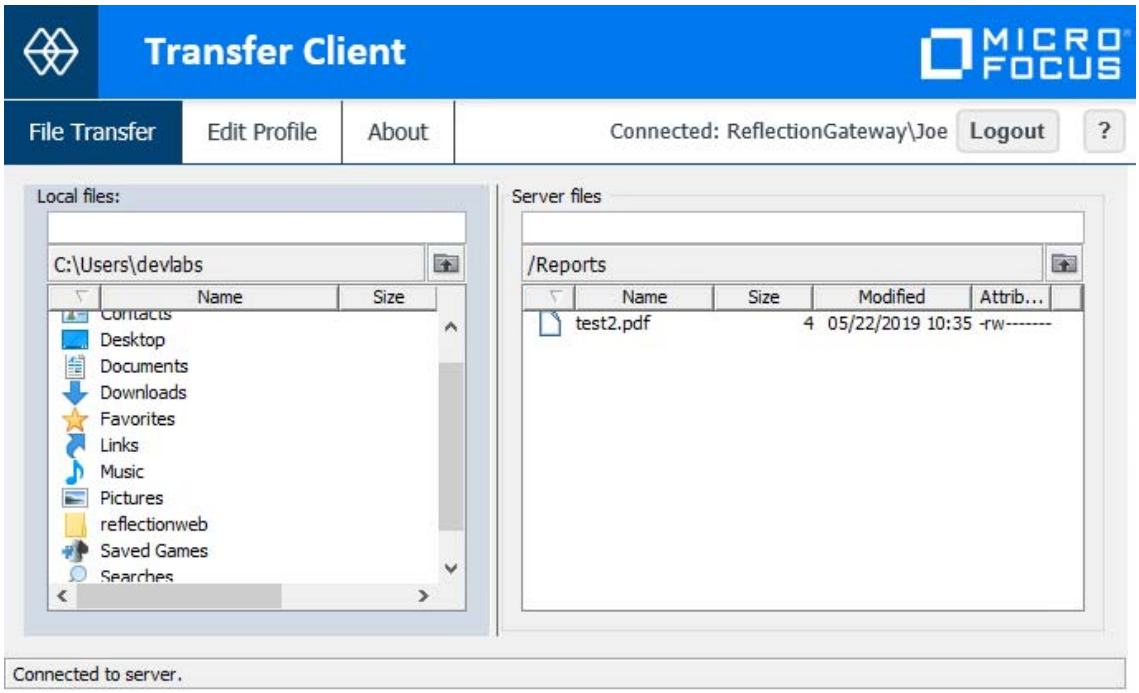
NOTE

- If the link doesn't work, confirm that it is pointing to your host and not the default (localhost). If your link points to localhost, see "Set Up Email" on page 17.
- You can also connect directly to the Transfer Client from a browser by pointing to your server at port 9492, as shown here: `https://GatewayServer:9492`. You can use this option if your default browser is not Java-enabled or to test from another system.

3 Log in as *Joe*.

Because the Transfer Server sends a self-signed certificate you'll see a certificate warning presented by the browser. Java also presents confirmation dialog boxes.

A successful connection shows your local files on the left and the contents of your Reports directory on the right.



4. Use the drag-and-drop interface to experiment with downloading and uploading files. Because of the permissions you set for Joe, only the downloads will succeed.
5. Click **Logout** to prepare for the next test.

Test the Complete File Transfer Pathway

At this point, Don has created a Job that monitors the Reports directory on an internal server and transfers PDF files from this server to a Reports directory on the Transfer Site server. He has also configured a Transfer Site that makes these files available to Joe. In this test you'll trigger this series of events by adding a new PDF file to the scanned directory.

Before you begin

- Confirm that your Reports Job is enabled and set to scan every minute.

Confirm that new reports are available to the customer

1. On the Reports server, put a new *.pdf file in `c:\reports`.
2. After a few minutes, check the email address you used for Don. Look for the Job Success notification that indicates that the new file triggered a successful Job.
3. Log into the Transfer Client as Joe. You should be able to see and download the new file.

5 Delegated Administration

Smart companies are paying increasing attention to secure internal management practices. With this in mind, Don wants to ensure that users with access to Gateway Administrator have access to only those features and servers they need to do their Job. For this, he will add delegated administrators and configure their access rights.

Set Up Delegated Administration

Lee is a financial analyst in Don's company. Don wants her to be able to add and edit Jobs and Transfer Sites, but does not want her to have access to Gateway Administrator system settings.

Add a File Transfer Administrator to Gateway Administrator

1. Log into Gateway Administrator as *Don*.
2. On the **Users** tab, click **New**.
3. For **UserID** enter *Lee*.
4. For **Email address**, you use an arbitrary address (like Lee@demo.com). The tests that follow don't use emails.
5. Click **Specify password**, then enter and confirm a password.
6. From the Reflection Gateway group membership list, select **File Transfer Administrators**.

   This group provides access to Transfer Sites, Jobs, and users, but not groups or system management.
7. Click **Save**.
8. Click **Logout** and log in as *Lee*. Notice that only four tabs are available to this user: **Transfer Sites**, **Jobs**, **Users**, and **About**.
9. Click **Transfer Sites**. Note that Lee does not yet have access to the site Don created. Transfer Sites can only be viewed and edited by individuals who are members of the Transfer Site and have management rights .
10. Click **Jobs**. Lee can see the Jobs Don created. Transfer Site Administrators have the Manage Jobs role enabled, and every user with this role can see all configured Jobs.
11. Click **Logout**.

You can use the next procedure to give Lee access to Don's Transfer Site.

Enable an additional user to Manage your Transfer Site

1. Log into Gateway Administrator as *Don*.
2. On **Transfer Sites** tab, select the *Reports* site and **Edit**.
3. Under **Existing User**, search for *Lee* and click Add.
4. In the user list for Lee, under **Permissions**, click the gear icon to change it from gray (disabled) to green (enabled). This gives Lee management rights to this site.

5 Click **Save**, then **Logout**.

6 Log in as *Lee*.

7 Click **Transfer Sites**. This user can now view and edit the Reports site.

8 Click **Logout**.

File server groups are a feature of the Gateway Administrator that enables you to specify which file servers Gateway Administrator users have access to. Use the next procedure to see how this feature works.

Use File Sever Groups to limit access to added file servers

1 Log into Gateway Administrator as *Don*.

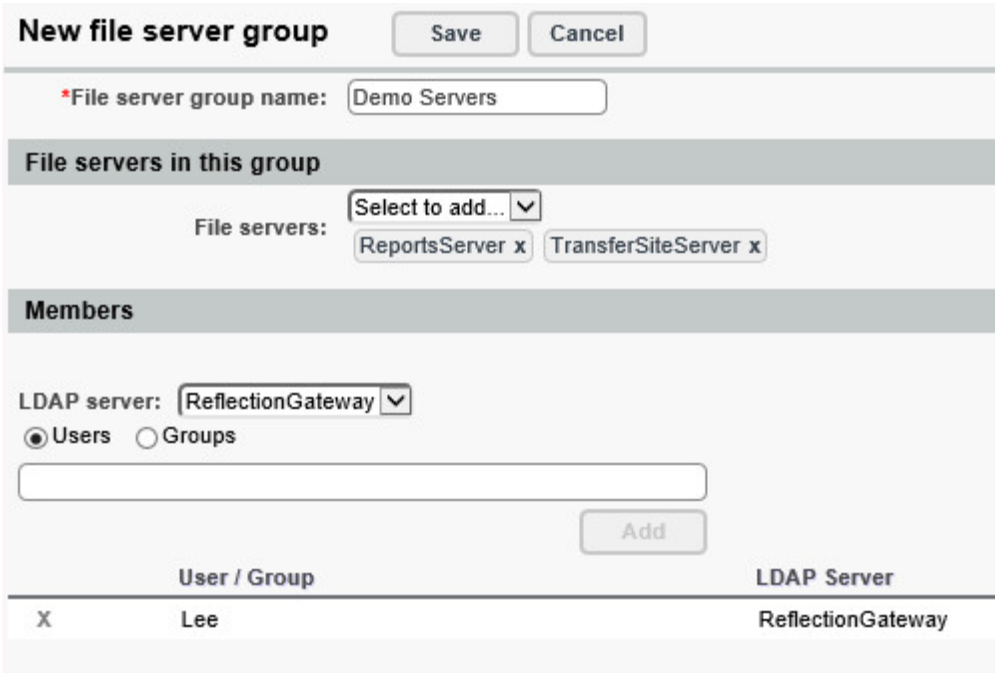
2 Go to **System** > **File Server Groups** > **New**.

3 For File server group name enter *Demo Servers*.

4 Use the **File servers** drop-down to add both of your file servers to this group.

5 Add *Lee* as a member of this group.

6 Click **Save**.



7 Click **Users** and add a new user, Paul. Use an arbitrary email and specify a password.

8 Add this user to the **File Transfer Administrators** group and click **Save**.

9 Log out, then log in as *Paul*.

10 On the **Jobs** tab, Paul cannot see the existing Jobs. This is because their actions require access to servers in the Demo Servers file server group, and he is not a member. If he tries to create a new Job, he sees a message telling him that he cannot create a Job because he doesn't have access to any servers.

11 Log in as *Lee* to confirm that–as a member of the Demo Servers group–she can view the existing Jobs and create new Jobs using the servers in this group. Click **Logout**.

12 Log in as *Don*. Although he is not a member of the Demo Serves group, he can view the existing Jobs and create new ones. This is because all users in the Administrators groups have access to all file servers regardless of how the file server groups are set up.

13 While you're still logged in as Don, delete the Demo Servers group. (Go to **System** > F**ile Server Groups**. Select the Demo Servers group and click **Delete**.)

When there are no file server groups configured, all users with Manage Jobs role can create and edit Jobs using all added servers.

14 Log out and log in again as *Paul*. Confirm that he can now view the existing Jobs and add new ones.

6 Transfer Auditing

The new security policy in Don's company requires a full, detailed audit log of all transferred files. He can use audit logging to maintain a record of file transfer activity.

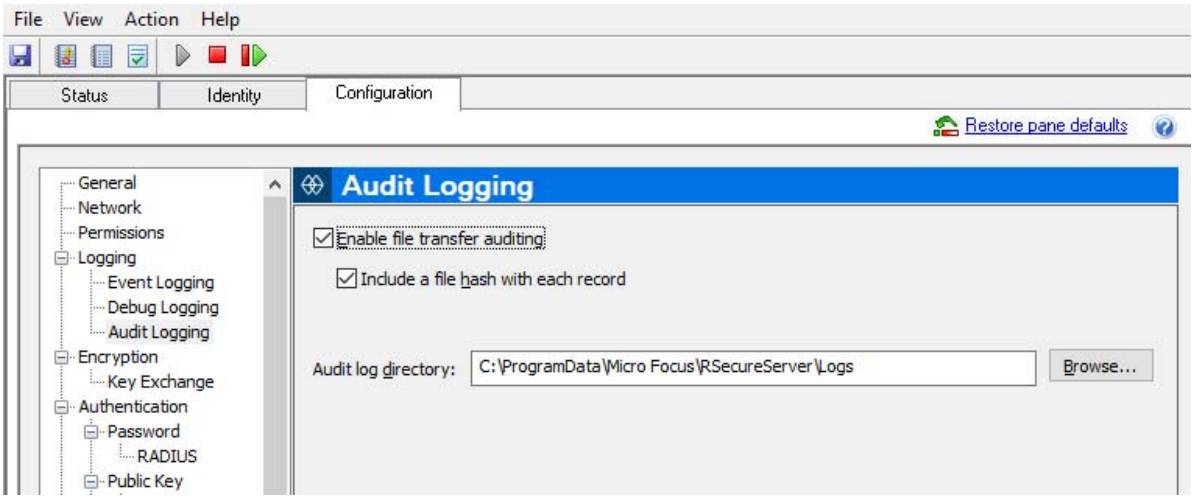
- To audit Transfer Site activity, set up audit logging on the Reflection Secure Shell Proxy.
- To audit Job actions that transfer files, set up audit logging on added Reflection for Secure IT Servers.

NOTE: Both Reflection for Secure IT Server for Windows and Reflection for Secure IT Server for UNIX support audit logging. The procedure below shows how to configure auditing in Reflection for Secure IT Server for Windows. If you decide to use a Reflection for Secure IT Server for Windows for UNIX, you can use the AuditLog keyword to enable audit logging. See the Reflection for Secure IT Server for UNIX User Guide (https://www.attachmate.com/documentation/rsit-unix-802/rsit-unix-guide/data/t_31076.htm) for details.

To enable file transfer auditing on Reflection servers for Windows

Use this procedure to enable audit logging on the Reflection Secure Shell Proxy or the Reflection for Secure IT Server for Windows.

1. As a Windows administrator on the system where you want to enable auditing, launch the Reflection console:
   - To set up Transfer Site auditing, start the Reflection Secure Shell Proxy. For this evaluation, the proxy is running on the same Gateway Server system that runs Gateway Administrator.
   - To set up auditing on the Reports server or the Transfer Site server, configure the Reflection for Secure IT Server for Windows running on those servers.
2. From the **Configuration** go to **Logging > Audit Logging**.
3. Select **Enable file transfer auditing**.
4. Save your settings (**File** > **Save Settings**).



To view a Transfer site audit log

1. Use the procedure above to enable audit logging on the Reflection Secure Shell Proxy.
2. Log into the Transfer Client as *Don* and transfer files in both directions.
3. From the Reflection Secure Shell Proxy console, use the audit log file toolbar button to view the audit log:

To view an audit log of transfers on the Reports server

1. Use the procedure above to enable audit logging in the Reflection for Secure IT Server for Windows running on your Reports server.
2. Add new PDF files to the scanned directory. Click **Run Now** from the Reports Job or wait for the scan interval.
3. From the Reflection for Secure IT Server for Windows console, use the audit log file toolbar button to view the audit log.